S. HRG. 108–951

REAUTHORIZATION OF THE FEDERAL TRADE COMMISSION (FTC)

HEARING

BEFORE THE

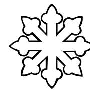
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JUNE 11, 2003

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

81–138 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JOHN McCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON H. SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire

ERNEST F. HOLLINGS, South Carolina, *Ranking*
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*
KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*
GREGG ELIAS, *Democratic General Counsel*

SUBCOMMITTEE ON COMPETITION, FOREIGN COMMERCE, AND INFRASTRUCTURE

GORDON H. SMITH, Oregon, *Chairman*

CONRAD BURNS, Montana
SAM BROWNBACK, Kansas
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
JOHN E. SUNUNU, New Hampshire

BYRON L. DORGAN, North Dakota, *Ranking*
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey

CONTENTS

	Page
Hearing held on June 11, 2003	1
Statement of Senator Dorgan	2
Statement of Senator Lautenberg	40
Statement of Senator Nelson	3
Statement of Senator Smith	1
Statement of Senator Wyden	2

WITNESSES

Cooper, Scott, Manager, Technology Policy, Hewlett-Packard Company	66
Prepared statement	67
Deutsch, Sarah, Vice President and Associate General Counsel, Verizon Communications	56
Prepared statement	57
Grant, Susan, Director, National Fraud Information Center/Internet Fraud Watch, National Consumers League	53
Prepared statement	54
Leary, Hon. Thomas B., Commissioner, Federal Trade Commission	10
Prepared statement of the Federal Trade Commission	11
Muris, Hon. Timothy, Chairman, Federal Trade Commission	3
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center (EPIC); Adjunct Professor, Georgetown University Law Center	46
Prepared statement	48
Sarjeant, Lawrence E., Vice President Law and General Counsel, United States Telecom Association (USTA)	59
Prepared statement	61
Schwartz, Ari, Associate Director, Center for Democracy and Technology	75
Prepared statement	76
Swindle, Hon. Orson, Commissioner, Federal Trade Commission	8
Thompson, Hon. Mozelle W., Commissioner, Federal Trade Commission	5

APPENDIX

Burns, Hon. Conrad, U.S. Senator from Montana, prepared statement	87

REAUTHORIZATION OF THE FEDERAL TRADE COMMISSION (FTC)

WEDNESDAY, JUNE 11, 2003

U.S. SENATE,
SUBCOMMITTEE ON COMPETITION, FOREIGN COMMERCE,
AND INFRASTRUCTURE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3:07 p.m. in room SR–253, Russell Senate Office Building, Hon. Gordon H. Smith, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Senator SMITH. Ladies and gentlemen, let the hearing come to order, and I apologize for the delay. I think you are probably all aware that we are in the midst of a series of roll-call votes. But in the interest of time, in the interest, frankly, of all the very accomplished witnesses who have assembled here today, I thought it well that we at least get going. And I want to welcome my colleague from Oregon, Senator Wyden, who is here. And hopefully, between these opening statements and the next vote, we can keep someone here to keep this hearing going forward. But again, I thank all of our witnesses, who have made, many of them, special arrangements to be here today.

The purpose of this hearing is to examine the performance of the Federal Trade Commission in fulfilling its mission, and to discuss legislative proposals for reauthorization.

The FTC is vital to ensuring fair treatment for American consumers in the marketplace. However, the Commission has not been reauthorized since 1996. I am pleased to say that, earlier today, Chairman John McCain and myself introduced the Federal Trade Commission Reauthorization Act of 2003. Now, we hope to consider the legislation during the Committee's executive session next week. Therefore, today's hearing is very timely, indeed.

The bill would authorize funding for the FTC for Fiscal Years 2004 through 2006. It also includes a number of provisions requested by the Commission. Among other things, it would enable the FTC to accept reimbursement from law enforcement agencies for investigative or other services provided in assistance by the FTC.

The bill also provides the FTC enhanced authority to respond to ever-growing international consumer fraud by allowing improved cross-border fraud action. Specifically, the FTC has requested,

among other things, that it be able to more readily exchange information with its foreign counterparts, seek redress on behalf of foreign consumers for U.S.-based fraud, make criminal referrals, delay notice to perpetrators of fraud in certain circumstances, and assist the Justice Department in foreign suits relevant to the FTC's interest. I look forward to further exploring this complex issue during today's hearing.

In addition to the provisions in the bill, this hearing will also address the FTC's request for the repeal of the common-carrier exemption in the Commission's organizing statute. This exemption currently blocks the Commission from exercising authority over certain activities of telecommunication's common carriers. I know that this issue involves a wide range of views, and I am hopeful that the Subcommittee will learn more from those appearing today.

And again, we thank our witnesses who are here, and I am pleased to be joined by the Ranking Member of this Subcommittee, Senator Dorgan. Senator Dorgan, please proceed if you have an opening statement, then Senator Wyden and Senator Nelson. Welcome, gentlemen.

STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, thank you very much. I think, because of the time, we have another vote that will be starting soon, and these interruptions make it very difficult to complete a hearing. Because of the time, let me just say this. The FTC is a very, very important Federal agency. They are working on a lot of interesting and very important issues—the Do Not Call Registry, the cross-border fraud, spam. I am interested in the common-carrier exemption. There are a series of things that are really very important for us to consider. Let's proceed to the hearing.

Senator SMITH. Thank you, Senator Dorgan.

Senator Wyden.

STATEMENT OF HON. RON WYDEN, U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you, Mr. Chairman. I, too, will be very brief. And there are a lot of topics to cover, but I want to touch on two, in particular.

First, on the issue of spam. Gentlemen, I believe that the U.S. Senate is going to pass a bill on this topic. I think it will involve having a tough national standard, with respect to discouraging the scourge of spam that really is threatening to poison the medium. But the real challenge is—and the Burns-Wyden legislation, of course, has penalties in it, criminal penalties, civil sanctions—the real challenge is to make sure the Federal Trade Commission enforces what the U.S. Congress does, because unless there is a very tough enforcement message sent, you are really going to find it very hard to deal with this problem. And I am particularly anxious to hear the Commission describe what the strategy is to enforce efforts to stem this flow of spam. There is some limited authority now. We seek to expand it. And I am anxious to hear the Commission's views on that.

Also, as Mr. Muris knows, I would like to know at what point the Commission is going to get serious about taking action to protect consumers in the energy market. If you look at the first quarter of 2003, gasoline prices spiked to record levels, the Big 5 oil companies recorded huge profits of $20 billion. These are profits that were more than three times higher than the first quarter of last year. I have been trying to find out what the Federal Trade Commission wishes to do to promote competition in this area for well over a year. And in response to my requests, I have gotten back a bunch of newspaper articles saying that essentially all these price spikes are due to refinery fires. I would hope that there would be a formal proposal forthcoming at some point to actually produce some competition in the energy business, and I hope that we will hear some efforts are underway at the Commission to do that now.

Mr. Chairman, I thank you.

Senator SMITH. Thank you, Senator Wyden.

Senator Nelson.

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman. And I want to thank you for your participation in that rather lengthy but very insightful hearing that we had on the spam legislation. And it is my understanding next week that the Committee is going to mark up the Wyden bill, and I have had the privilege of participating with them and will have some modest amendments to strengthen portions of it. But I would just underscore what Senator Wyden said, that the FTC's vigilance in making it happen, as a regulator, would be very important for consumers.

Furthermore, I am interested in pursuing your ideas on consumer credit reporting and whether or not there are audits to make sure that the consumer credit reporting is accurate. I hear examples back in my State of Florida where there is not the accuracy that one would hope for. And a lot of financial decisions ride on the accuracy of those credit reports.

So, again, I thank you all for your public service. I think you have done a fine job. I think we have got a lot of work, and a lot of it we can do together.

Thank you, Mr. Chairman.

Senator SMITH. Thank you, Senator Nelson.

We are pleased that our first panel consists of our FTC Commissioner, the Honorable Tim Muris, Chairman. And he is joined by Commissioners Mozelle Thompson, Orson Swindle, and Thomas Leary. We thank you all, gentlemen, for being here. And I understand, Mr. Muris, you will lead off, and each of you will have comments.

STATEMENT OF HON. TIMOTHY MURIS, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. MURIS. Thank you very much, Mr. Chairman. We certainly appreciate the opportunity to testify today about our reauthorization.

On behalf of the Commission, let me first start by expressing our sincere thanks to you, Mr. Chairman, and all the Members of this Subcommittee, for your continued support of the agency.

Since our hearing last summer, our dedicated staff has continued to take innovative and aggressive actions to protect consumers and promote competition. I would like to briefly outline our mission and some of our recent accomplishments. My colleagues will then each discuss specific legislative proposals, some of which—well, in fact, all of which you have mentioned in your opening statements.

Our consumer-protection mission focuses on attacking fraud and deception, consumer privacy, deceptive lending practices, and cross-border law enforcement. This program provides Americans with impressive results. Since April 1st of 2002, we have organized 12 joint enforcement efforts, or sweeps, with more than 165 partners. These sweeps resulted in more than 400 cases, targeting Internet scams and telemarketing fraud, including deceptive work-at-home opportunities, deceptive health claims, advanced-fee credit-related fraud, fundraising fraud, and Internet auction fraud. Overall, since April 2002, we have obtained more than 65 final judgments, ordering more than $865 million in consumer redress.

In addition to attacking fraud, we devote significant resources to protecting consumer privacy. This year, with your assistance, we are set to launch the National Do Not Call Registry. Implementation of this registry will begin soon; and, once it is in place, consumers who have registered will begin to receive fewer and fewer unwanted telemarketing calls. I want to thank you, Mr. Chairman and this Committee, for your support of this important initiative.

In addition to unwanted telemarketing calls, unsolicited commercial E-mail, or spam, is a growing consumer concern. We are addressing consumer concerns about spam through law enforcement, consumer and business education, and research. In addition, the Commission has legislative ideas that Commissioner Swindle will discuss.

We have been equally as active protecting consumers from anti-competitive conduct that could raise prices, particularly in the healthcare, energy, and high-tech industries. In healthcare, a number of FTC activities will likely provide consumers with more affordable drugs. For example, we published a study examining the frequency of anti-competitive abuses to block market entry of low-cost generic drugs, provided comments to the FDA on the potential for misusing the Hatch-Waxman Act that governs generic entry, and we brought law enforcement actions against branded companies allegedly improperly delaying generic entry.

Recently, for example, we announced a settlement with Bristol-Meyers-Squibb concerning alleged abuses of the Hatch-Waxman process to obstruct the entry of generic competition for two anti-cancer drugs and an anti-anxiety agent. This case and our efforts, I believe, will save consumers tens, if not hundreds, of millions of dollars.

We have also been active in protecting consumers from anti-competitive conduct that may raise the price of oil and gas, and I certainly look forward to discussing this issue at more length with Senator Wyden.

We recently filed a complaint alleging that Unocal improperly manipulated the process through which California set regulations for the formulation of low-emissions gasoline. We have also, in the last year, begun a project that monitors wholesale and retail prices of gasoline in a real-time basis in approximately 360 cities across the United States, in an effort to identify possible anti-competitive activities.

We are also making several recommendations for legislative changes, and we would be very happy to work with you and your staff on these recommendations.

First, Commissioner Thompson will provide an overview of our recommendations to improve cross-border fraud enforcement. These proposals are also critical to the fight against deceptive spam, because spammers often send their messages from anywhere in the world to anyone in the world.

Second, Commissioner Swindle will discuss our recommendations to enhance the FTC's effectiveness in fighting fraudulent spam. These proposals would improve our ability to investigate and sue possible targets.

Finally, Commissioner Leary will discuss our recommendations to eliminate the FTC Act's exemption for communication's common carriers.

Thank you very much.

Senator SMITH. Thank you.

Gentlemen, do you desire to go vote now and then—take a short recess and come right back? OK.

Mr. Thompson, we will just sort of move in and out. OK. Mr. Thompson.

STATEMENT OF HON. MOZELLE W. THOMPSON, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. THOMPSON. Thank you.

Good afternoon, Mr. Chairman and Members of the Committee, and thank you for the opportunity to appear before you today and offer testimony in support of the FTC's reauthorization.

Last year, when I appeared before the Committee, I discussed the FTC's work in the area of international consumer protection. I noted, at that time, that improvements in communication and technology have created a global marketplace in which American consumers and American businesses play an important and active role. I also noted that these same improvements left American consumers open to new types of harm, and that these cases were growing at an exponential rate.

Today, I would like to talk about one of the most significant consumer-protection problems in the last several years—the globalization of fraud and deception, and the FTC's response—because not only has the consumer marketplace become global, so have the purveyors of fraud and deception.

As you can see from this chart, the same technological tools that have expanded markets across international boundaries have allowed fraudsters to act more efficiently and quickly to extend their reach beyond domestic markets. This shows you where some complaints from American consumers lie, these various countries listed

in blue. The FTC needs new tools to effectively combat cross-border fraud and deception, and we ask you for them today.

Now, there was a time not long ago when the biggest challenge to American consumers was whether they wanted to do business with the mail-order company on the other side of the country. Most of our consumer-protection laws are based on what we knew then, and they have served us well. Today, however, America represents the largest and richest consumer marketplace in the world. Improved technologies have opened world markets to American consumers, and vice versa, so it is not surprising that American consumers are bombarded with new opportunities to spend their money. These opportunities arrive from around the world via mail, telephone, television, and even spam. While many of these opportunities might be legitimate, a rapidly growing number are fraudulent and deceptive.

As you can see from this chart, what is contained in light blue is some of our complaint data. This large percentage, in light blue, is U.S. consumers' complaints against companies just located in Canada. The other, the dark blue, is U.S. consumers against companies located in other countries. This is a tremendous proportion of some of our cross-border complaints.

In response to this dramatic increase, the FTC has taken a leadership role in reaching a mutual understanding with our international colleagues that we must bring down barriers to prosecuting fraudsters who prey on victims across borders. Consumer-protection law enforcers around the world now agree that this problem is serious and that international cooperation is key to any effort to combat cross-border fraud and deception.

We work in a variety of international fora to address these problems. Our efforts have resulted in bilateral memoranda of understanding, and they include our participation in the International Consumer Protection Enforcement Network, or ICPEN, a group of consumer-protection law enforcement agencies from around the world.

The issue of cross-border fraud and deception is also at the forefront of the work that we do at the Organization for Economic Cooperation Development, or OECD, Committee on Consumer Policy. That Committee, which I chair, has worked to develop guidelines that provide the 30 OECD Governments with a blueprint for cooperation in combating cross-border fraud. We hope that these guidelines will be finalized and approved later this month. But our participation in these international fora are not enough.

Criminal law enforcers saw the need for international cooperation a long time ago. They found ways to permit Government authorities to share investigatory materials and to engage in cooperative law enforcement. Later, the Federal Government recognized the negative market impact of such activities as securities and commodities fraud. Consequently, agencies such as the SEC and the CFTC were given certain powers that enable them to better prosecute such frauds across national borders.

Unlike our sister agencies, the FTC's tools to combat fraud and deception have simply not caught up with the times. In many instances, the statutes under which we operate do not address the in-

creasingly cross-border nature of fraud and deception, and sometimes even hinder our ability to engage in such activity.

The growth of cross-border fraud demonstrates the pressing need for new tools. Our statistics show a sharp increase in the number of cross-border complaints from American consumers about foreign companies, from 7,600 or so in 1998 to 24,213 in calendar-year 2002. And you can see that from this exhibit, Exhibit 3. And in fact, just from 2001 to 2002, the number of complaints almost doubled.

Even at our recent Spam Forum——

Senator DORGAN. Mr. Thompson, may I stop you on that point? With respect to the consumer complaints against companies located in foreign countries, can you give me a ballpark estimate of what percent of those come from Internet transactions or credit-card transactions, either one?

Mr. THOMPSON. I do not want to give you that off the top of our head. There is a large portion of them that are. The Internet has facilitated the growth of that kind of problem. But if you look the percentage that go across the border to Canada, a lot of that comes from television and phone solicitations. So I would want to be more precise in giving you a number, but the Internet has caused this to grow exponentially.

Senator DORGAN. I asked that question—I had two charges from a French company on a credit card about a year ago, and when I began checking into it, I was told, "Well, this company's name is well known, because they have done it many, many times." And so credit-card Internet transactions, I assume, are real locations for this sort of fraud. Is that right?

Mr. THOMPSON. Uh-huh. Well, it is no secret that our market is the richest market, so people want to come here to defraud our consumers. But right now, the way our laws are situated, that—we would have a difficult time sharing information about your complaint about a French company with French authorities; or, for that matter, if they were to prosecute a French company, and they knew that they had recovered funds that belong to you, they would have a hard time sharing that information with us, or for us to receive it, in order to get you your refund. That is because the way our law is situated, that it really is designed for a domestic market.

But if you look at what we are doing with spam, just because we see that so much of it comes from outside of our borders, for that reason alone, cross-border fraud legislation is necessary to make spam legislation effective.

Senator DORGAN [presiding]. Mr. Thompson, let me interrupt you and say I also am going to leave to go vote. Senator Wyden has voted and returned.

[Laughter.]

Senator DORGAN. I know that you may have taken it personally that you have driven most of the Members out of the room, but——

[Laughter.]

Senator DORGAN.—but we actually have a vote, and that is why we are moving back and forth.

Mr. THOMPSON. People have said worse things to me.

Senator DORGAN. Anyway, your testimony is very interesting.

Senator Wyden?

Mr. THOMPSON. Well, I am just about ready to conclude.

Senator DORGAN. Why don't you proceed?

Mr. THOMPSON. The legislative proposal, in sum, that we have given to you is intended to address some of the problems that I have outlined and to improve our ability to protect consumers who are defrauded across borders. Quite simply, we are just asking for tools to make us more effective in meeting those new challenges.

So I am here to answer your questions about—and I will start all over again, Senator Wyden, if you want me to.

Senator WYDEN [presiding]. Very good. Commissioner Swindle, why don't we go to you next.

STATEMENT OF HON. ORSON SWINDLE, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. SWINDLE. Thank you, sir. Thank you, Mr. Chairman and Senator Wyden and Members of the Committee, for this opportunity to appear before you with Chairman Muris and my fellow Commissioners.

Today, I would like to briefly address a growing problem for all of us, the unsolicited commercial E-mail, or unwanted E-mail, or spam, as it has come to be known. Consumers must have trust and confidence in technology and its uses, particularly when it comes to the privacy and security of their personal and sensitive information. Spam undermines consumer trust and confidence, and it is a rapidly growing threat to Web-based services.

The Commission's testimony, provided in lengthy form to the Committee, provides the Committee with an overview of our efforts to combat spam and also legislative recommendations to address spam. The legislative recommendations are modeled after the Telemarketing Act. However, many of the Commission's recommendations are already contained in the Burns-Wyden Spam Bill. For example, like the Telemarketing Act, the Burns-Wyden bill provides for State law enforcement action in Federal court and allows collection of civil penalties. More details on procedural and substantive legislative proposals are addressed, as I mentioned, on pages 43 through 48.

Spam raises a number of concerns. The volume of spam is increasing at astonishing rates. In addition, recent Commission studies indicate that spam has become the weapon of choice for those engaged in fraud and deception. Spam also can transmit viruses, Trojan horses, and other damaging code capable of inflicting major damage on the Internet and our critical infrastructure. These concerns represent enormous cost to the consumers, to businesses, and the economy.

There is no easy solution to the spam problem, certainly no single approach that will solve the problem. Nevertheless, spam raises problems that demand attention by policymakers and industry leaders. First, there is a complex combination of technology, market forces, and public policy that will be evolving for years to come.

In addition, the spam problem is heavily influenced by the emotions of millions of computer users, who are literally fed up with spam. Spam is about to kill the killer app of the Internet—that is, the use of E-mail and E-commerce. If consumers lose trust and confidence in Web-based services and stop using them as tools for com-

munication and online commerce, tremendous harm will be done to the economic potential of information technology.

Solving these problems requires innovation, resources, and time. However, dealing with the emotional reaction of spam by millions of users requires our immediate attention before it gets out of hand. Internet-service providers, software manufacturers, and those engaged in designing operating systems must empower consumers with better control over their incoming E-mail.

Easing the spam burden on consumers would help to shore up trust and confidence. Surely this is possible right now. Why has the industry not done so? Frankly, I am not convinced that industry really wants to empower consumers by giving them easy-to-use tools to control their incoming E-mail. Spam is a crisis today. We need great minds to quickly find solutions. Empowering consumers would be a very good first step. Industry must do this, and it must do it now.

The Commission will continue its multifaceted efforts to address spam. For example, the Commission will continue—and I must repeat, will continue—its aggressive law enforcement program against deceptive spam. However, it is both resource intensive and technically challenging to find the guilty parties.

Consumer education and awareness are also essential. Our website, *www.ftc.gov/infosecurity,* our consumer outreach, and partnerships with industry on fighting spam and promoting safe computing, are expanding our reach.

The Commission also conducts research on various aspects of spam. Three recent Commission studies helped us to better understand the magnitude of deceptive spam and how consumers are victimized. The Commission's Spam Forum, in May, was intended to better inform the dialogue and to explore possible solutions to spam. The forum was remarkable in its discussions and participation. Over 80 panelists and 400 people attended the conference.

I would like to share some of the forum's revelations about the realities of spam. First and foremost, the private sector must lead the way to finding solutions to spam. We likely will not find the perfect solution. The target will be constantly moving as technology evolves. More laws are not necessarily the right answer. Laws bestowing a competitive advantage to larger firms over smaller firms are questionable. Unenforceable laws will have little real effect. Overreaching laws will unintended adverse consequences. Passing legislation to mandate best practices for good actors will not help us track down the bad actors engaged in fraud and deception. Industry, Government, consumers, and other end users in the civil society organizations must be a part of a continuing dialogue to find solutions.

In addition, consumer awareness and developing safe computing practices by all participants are essential. Developing a culture of security where all participants work to enhance consumer security and minimize the vulnerabilities to the Internet and our critical infrastructure is an imperative, not an option.

The effort to solve the spam problem and secure our information systems and networks is a journey, not a destination, and we have miles to go before we sleep.

Thank you very much, Mr. Chairman.

Senator SMITH [presiding]. Thank you very much. Mr. Leary.

STATEMENT OF HON. THOMAS B. LEARY, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. LEARY. Mr. Chairman and Members of the Subcommittee, my role here today is to present, once again, our unanimous recommendation that the Federal Trade Commission Act be amended to eliminate the special exemption for telecommunication's common carriers. We want to thank the Committee for acting favorably on this recommendation last year when you reported out S. 2946. We have also noted the concerns expressed by some Members on this issue, and I intend to say something about these concerns this afternoon.

When the common-carrier exemption was included in the FTC Act many years ago, the exemption made sense. It was logical to exempt the monopoly providers of common-carrier services who were not disciplined by competition, but rather by detailed rate and service regulation. Since that time, the telecommunications industry has changed dramatically, and, perhaps even more important, the regulatory role of the Federal Government has also changed dramatically.

Let me summarize some of the changes that are particularly significant.

One, the common-carrier activities of telecom companies are less regulated by Government fiat and more by competition today. At the same time, telecom companies have been allowed to expand into non-common-carrier activities, like Internet services. They provide these services in competition with companies that are unqualifiedly subject to our jurisdiction.

Two, over the last century, you have passed myriad laws and regulations, and created entirely new agencies to monitor and regulate specific activities of business enterprises, whether they are common carriers or not. Sector-specific regulation of the kind that the FCC or the FDA provides has been supplemented everywhere by specific substantive law enforcement of agencies like the SEC, OSHA, or the EPA, agencies that, like the FTC, have a broad jurisdiction over a large number of sectors, but monitor a limited range of activities in any one sector.

Three, we, in the FTC, have, therefore, a long experience cooperating with other agencies to avoid duplication or inconsistency in these situations. Specifically, we want to cooperate with the FCC, and we have no ability or desire to intrude into the FCC's core mission as gatekeeper into the limited-communications spectrum. We do not make the same kinds of public-interest determinations that they do. We are not concerned with the qualifications of companies that compete, or the nature of services that they provide. The core mission that you have assigned to us is to see that any company, whatever it does, conducts its business with fairness and with honesty. In carrying out that mission, we have acquired an in-house expertise and a body of precedents that I really believe are unmatched anywhere in this country or, indeed, the world.

Now, some ask why we are asking for change after all these years, and that is a fair question. The short answer is, that technologies are continually converging, and we have become increas-

ingly frustrated by our inability to obtain complete relief in situations where: (a) there are multiple parties, some of whom are common carriers and some of whom are not, (b) where a common carrier engages in deceptive practices involving a mix of common-carrier and non-common-carrier activities, or (c) the jurisdiction lines are unclear, and resources are wasted dealing with an issue that has nothing to do with the merits. Finally, an admitted common carrier may engage in deceptive practices that are similar to those we see all the time that do the same consumer harm and for which we have special remedies, but we are paralyzed by the jurisdictional barrier.

Potential agency overlaps may require discussion and cooperation. We have had an ongoing exchange with the FCC on this subject. I want to thank Senator McCain and his staff particularly for facilitating discussions on how to make a shared jurisdiction effective. We want to avoid duplicative efforts, but we also want to remedy the present situation where companies engaged in the same conduct in competition with one another are subject to different regulatory regimes.

In conclusion, let me assure you that we do not want to intrude into other agencies' business, and we do not seek to impose remedial relief absent a need for it. But you decided, long ago, that the issues we are talking about here are our business, and we cannot do the best possible job for consumers, whom we both seek to serve, while we are constrained by a barrier that has long outlived its usefulness.

Thank you very much.

[The prepared statement of the Federal Trade Commission follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Mr. Chairman, the Federal Trade Commission ("Commission" or "FTC") is pleased to appear before the Subcommittee today to support the FTC's reauthorization request for Fiscal Years 2004 to 2006.[1] Since the last reauthorization hearing, the FTC has continued to take innovative and aggressive actions to protect consumers and promote competition. The Commission would like to thank the Chairman and members of the Subcommittee for their continued support of the agency's missions.

Introduction

The FTC acts to ensure that markets operate efficiently to benefit consumers. The FTC's twin missions of competition and consumer protection serve a common aim: to enhance consumer welfare. The FTC's competition mission promotes free and open markets, bringing consumers lower prices, innovation, and choice among products and services. The FTC's consumer protection mission fosters the exchange of accurate, non-deceptive information, allowing consumers to make informed choices in making purchasing decisions. Because accurate information in the marketplace facilitates fair and robust competition, the FTC's twin missions complement each other and maximize benefits for consumers.

Five principles guide the FTC's agenda for consumers. In exercising its competition and consumer protection authority, the FTC:

- Promotes competition and the unfettered exchange of accurate, non-deceptive information through strong enforcement and focused advocacy;
- Stops conduct that poses the greatest threat to consumer welfare, such as anticompetitive agreements among rivals and fraudulent and deceptive practices;

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any other Commissioner.

- Employs a systematic approach for identifying and addressing serious misconduct, with special attention to harmful behavior in key economic sectors;
- Uses the agency's distinctive institutional capabilities by applying its full range of tools—prosecuting cases, conducting studies, holding hearings and workshops, engaging in advocacy before other government bodies, and educating businesses and consumers—to address competition and consumer protection issues; and
- Improves the institutions and processes by which competition and consumer protection policies are formulated and applied.

During the past year, the FTC has applied its unique complement of law enforcement and policy instruments to address critical consumer concerns. Highlights include:

- *Privacy: "Do-Not-Call."* The Commission promulgated far-reaching amendments to its Telemarketing Sales Rule ("TSR"). Among the most important changes, the agency is poised to launch its National Do-Not-Call registry, one of the most significant consumer protection initiatives in recent years. The registry will be a central database of telephone numbers of consumers who choose not to receive telemarketing calls. Once the registry is in place this summer, telemarketers will pay a fee to gain access to the registry and then must scrub their telemarketing lists against the telephone numbers in the database. This fall, consumers who have placed their telephone numbers on the registry will begin to receive fewer and fewer unwanted telemarketing calls.
- *Health Care: Prescription Drugs.* Medical therapy increasingly relies on new pharmaceuticals as alternatives to more invasive treatments, such as surgery. A number of FTC activities will likely, directly or indirectly, help consumers to afford drugs to meet their needs. The FTC published a study examining the frequency of anticompetitive abuses to block market entry of lower-cost generic drugs; provided comments to the Food and Drug Administration ("FDA") on the potential for misusing the Hatch-Waxman Act procedures governing generic entry; and brought law enforcement actions against branded drug companies alleging improper efforts to delay generic entry. Among other significant matters, the Commission reached a settlement with Bristol-Myers Squibb ("BMS") resolving charges that BMS abused the Hatch-Waxman process to obstruct the entry of generic competition for two anti-cancer drugs and an anti-anxiety agent.
- *Financial Practices: Fraudulent Lending.* In May 2003, the court finalized a settlement to resolve FTC charges that The Associates (now owned by Citigroup, Inc.) had engaged in widespread deceptive and abusive practices involving subprime home mortgage lending. The settlement is expected to provide $215 million in redress through cash refunds and reduced loan balances to approximately 2.2 million consumers in the U.S., Puerto Rico, and the Virgin Islands. A related class action settlement is expected to yield an additional $25 million, for total relief to consumers of $240 million.
- *E-Commerce: A Unified Approach to Maintaining Efficient Markets.* The development of the Internet has created a host of consumer issues, requiring the FTC to draw on all its consumer protection and competition capabilities. Among other activities, the FTC has formed an Internet Task Force to analyze state regulations that may restrict the entry of new Internet competitors; hosted public workshops on both spam and potential anticompetitive barriers to e-commerce; and brought significant law enforcement actions that continue its historical role of leading efforts to keep e-commerce free from fraud, deception, and unfair or anticompetitive practices.
- *Energy: Gasoline.* In an administrative complaint issued in March 2003, the FTC alleged that Unocal improperly manipulated the process through which the California Air Resources Board set regulations for the formulation of low-emissions gasoline. The FTC contended that Unocal's anticompetitive conduct potentially could cost California consumers hundreds of millions of dollars per year in higher gasoline prices.
- *Innovation: Intellectual Property and Competition.* With the growth of the knowledge-based economy, the relationship between competition and patent policy as spurs to innovation has become increasingly important. The FTC, together with the Antitrust Division of the Department of Justice, held hearings over 24 days, with more than 300 participants, to explore this topic. A report will issue later this year.

In the next two years, the FTC will continue to address significant law enforcement and policy issues and to devote its resources to those areas in which it can have a major impact on behalf of consumers. With respect to the consumer protection mission, the focus will be on broad efforts to fight fraud and deception, as well as on consumer privacy and security initiatives, including efforts to address spam and ID theft. With respect to the competition mission, the FTC will continue merger and nonmerger policy development and law enforcement, with particular emphasis on health care, energy, high technology, and international issues.

This testimony addresses areas of FTC focus with discussions of specific activities and accomplishments on behalf of consumers. To further improve the FTC's ability to implement its mission and serve consumers, this testimony concludes with legislative recommendations to (1) eliminate the FTC Act's exemption for communications common carriers, (2) enact measures to improve the FTC's ability to combat cross-border fraud, (3) enact measures to improve the FTC's ability to combat spam, and (4) make technical changes to allow the agency to accept reimbursements and certain gifts and services that can enhance our mission performance.

II. Consumer Protection

A. Fraud and Deception

The FTC targets the most pervasive types of fraud and deception in the marketplace, drawing substantially on data from Consumer Sentinel, the agency's award-winning consumer complaint database,[2] and from Internet "surfs" that focus on specific types of claims or solicitations that are likely to violate the law. Since April 1, 2002, the FTC has organized 12 joint law enforcement efforts ("sweeps") with more than 165 law enforcement partners.[3] These sweeps resulted in more than 400 law enforcement actions targeting Internet scams and telemarketing fraud, including deceptive work-at-home opportunities, deceptive health claims, advance-fee credit-related fraud, fundraising fraud, and Internet auction fraud. The FTC filed 70 of these law enforcement cases.

Overall, since April 2002, the FTC has filed more than 145 cases involving fraud or deception and has enjoyed significant success in obtaining redress orders to provide relief for defrauded consumers, with more than 65 final judgments to date ordering more than $865 million in consumer redress.[4] The agency continues to ensure compliance with district court orders by bringing civil contempt proceedings when appropriate, and by assisting in criminal prosecution of FTC defendants who flagrantly violate court orders.

The FTC's actions against fraud and deception directly affect consumers. For example, in November 2002, the FTC finalized a consent order against Access Resource Services, Inc. and Psychic Readers Network, the promoters of "Miss Cleo" psychic services, who allegedly engaged in deceptive advertising, billing, and collection practices. The defendants stipulated to a court order requiring them to stop all collection efforts on accounts against consumers who purchased or purportedly purchased defendants' pay-per-call or audiotext services, to pay $5 million in equitable relief, and to forgive an estimated $500 million in outstanding consumer charges.[5]

In January 2003, the FTC obtained a permanent injunction against SkyBiz.com, Inc., an alleged massive international pyramid scheme. The final settlement includes $20 million in consumer redress to be distributed to both domestic and foreign victims. The settlement also bans the principal individual defendants from multi-level marketing for a period of years.[6]

In March 2003, the FTC announced settlements with five individual defendants who allegedly engaged in deceptive charitable telemarketing by misrepresenting both the charities that donations would benefit and the percentage of donations that

---

[2] In 2003, Consumer Sentinel was named one of the top 25 E-Government programs by the Industry Advisory Council and the Federal Chief Information Officer Council.

[3] The FTC works with various Federal and state law enforcement agencies, as well as Canadian, Mexican, and other international authorities. *See, e.g.,* FTC Press Release, *State, Federal Law Enforcers Launch Sting on Business Opportunity, Work-at-Home Scams* (June 20, 2002), available at *<http://www.ftc.gov/opa.2002/06/bizopswe.htm>*. *See also* FTC Press Release, *FTC, States Give "No Credit" to Finance Related Scams in Latest Joint Law Enforcement Sweep* (Sept. 5, 2002), available at *<http://www.ftc.gov/opa/2002/09/opnocredit.htm>*.

[4] This figure represents the amount of redress that has been ordered by the courts in more than 65 orders from April 2002 to May 2003. The figure does not represent the actual amount of money that has been or will be collected pursuant to those orders.

[5] *FTC* v. *Access Resource Services, Inc.,* Civ. Action No. 02–60226–CIV Gold/Simonton (S.D. Fla. Nov. 4, 2002).

[6] *FTC* v. *SkyBiz.com, Inc.,* Civ. Action No. 01–CV–396–EA (M) (N.D. Okla. Jan. 28, 2003).

the charities would receive.[7] Between 1995 and early 1999, the defendants raised more than $27 million. Among other terms of the settlements, defendant Mitchell Gold is subject to a $10 million judgment. Following an FTC criminal referral, Gold was indicted for mail and wire fraud in connection with the fundraising business and another fraudulent telemarketing scheme. Gold pled guilty and was sentenced to 96 months in prison.

B. Consumer Privacy

The FTC will continue to devote significant resources to protecting consumer privacy. Consumers are deeply concerned about the security of their personal information, both online and offline. Although these concerns have been heightened by the rapid development of the Internet, they are by no means limited to the cyberworld. Consumers can be harmed as much by the thief who steals credit card information from a mailbox or from a discarded billing statement in the trash as by one who steals that information over the Internet. Of course, the nature of Internet technology raises its own special set of issues.

1. Do-Not-Call. As highlighted above, the FTC has initiated a national Do-Not-Call registry, a centralized database of telephone numbers of consumers who have asked to be placed on the list. The Do-Not-Call registry—part of the FTC's 2002 amendments to the TSR—will help consumers reduce the number of unwanted telemarketing phone calls.

2. Identity Theft. The FTC's toll-free number 1–877–ID–THEFT is the Nation's central clearinghouse for identity theft complaints. Calls regarding identity theft have increased from more than 36,000 calls in FY 2000 to more than 185,000 calls in FY 2002. These complaints are available to the FTC's law enforcement partners through an online database, and now more than 620 law enforcement agencies can access this data. In addition, FTC investigators, working with the Secret Service, develop preliminary investigative reports that are referred to regional Financial Crimes Task Forces for possible prosecution.

Continuing a program begun in March 2002, the FTC, the Secret Service, and the Department of Justice ("DOJ") conduct training seminars to provide hundreds of local and state law enforcement officers with practical tools to combat identity theft. To date, the FTC and its partners have conducted six regional training sessions for 620 law enforcement officers.

The FTC also engages in extensive education of both businesses and consumers about preventing and responding to identity theft. One of the agency's most popular publications is "Identity Theft: When Bad Things Happen to Your Good Name."[8]

3. Safeguarding Consumer Information. In May 2002, the FTC finalized an order settling charges that Eli Lilly & Company unintentionally disclosed e-mail addresses of users of its *Prozac.com* and *Lilly.com* sites as a result of failures to take reasonable steps to protect the confidentiality and security of that information. The settlement requires Lilly to establish a security program to protect consumers' personal information against reasonably anticipated threats or risks to its security, confidentiality, or integrity.[9]

In December 2002, the FTC settled charges against Microsoft Corporation that, among other things, the company misrepresented the measures it used to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport web services.[10] Microsoft has agreed to implement a comprehensive information security program for Passport and similar services. The FTC will continue to bring actions involving claims deceptively touting the privacy and security features of products and services, as well as failures to maintain adequate security for personal information.

In May 2002, the Commission finalized its Safeguards Rule to implement the security provisions of the Gramm-Leach-Bliley Act ("GLB").[11] The Rule establishes standards for financial institutions to maintain the security of customers' financial information, and became effective in May 2003. To help businesses comply with the Rule, the agency issued a new business education publication, and will conduct

---

[7] *FTC* v. *Mitchell Gold,* Civ. Action No. SAcv 98–968 DOC (Rzx) (C.D. Cal. Mar. 7, 2003).

[8] Since the FTC first published the booklet in February 2002, the FTC has distributed more than 1.2 million paper copies and logged more than 1 million "hits" accessing the booklet on the FTC website. The publication is available at <*http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm*>.

[9] *Eli Lilly & Co.,* Dkt. No. C–4047 (May 10, 2002).

[10] *Microsoft Corp.,* Dkt. No. C–4069 (Dec. 24, 2002).

[11] Standards for Safeguarding Customer Information; Final Rule, 67 Fed. Reg. 36,484 (May 23, 2002) (to be codified at 16 C.F.R. Part 314).

other initiatives to inform businesses of the Rule and provide compliance guidance.[12]

Commissioner Orson Swindle, in particular, has focused on issues involving information security. During the past year, he has served as head of the U.S. delegation to the Organization for Economic Cooperation and Development ("OECD") Experts Group for Review of the 1992 OECD Guidelines for the Security of Information Systems. The group released revised guidelines in August 2002 that consist of nine principles promoting a "culture of security." The FTC has promoted the dissemination of these principles among industry and consumer groups. The FTC's consumer security website, <*www.ftc.gov/infosecurity*>, contains practical tips for staying secure online and features "Dewie the Turtle," a colorful cartoon mascot to promote effective online security. In addition, the FTC has worked with the White House Office of Cyberspace Security and the Department of Homeland Security to develop consumer awareness aspects of the National Strategy to Secure Cyberspace.

4. Children's Online Privacy Protection Act ("COPPA").[13] COPPA requires commercial websites to give notice of their information practices and to obtain parental consent before collecting, using, or disclosing personal information about children under the age of 13. Since April 2001, the FTC has brought eight COPPA cases and obtained agreements requiring payment of civil penalties totaling more than $350,000.[14] The two most recent cases involved settlements with Hershey Foods and Mrs. Fields.[15] Both companies agreed to settle charges that their websites allegedly collected personal data from children without complying with COPPA requirements.

5. Spam. The problems caused by unsolicited commercial e-mail ("spam")[16] go well beyond the annoyance spam causes to the public. These problems include the fraudulent and deceptive content of most spam messages, the sheer volume of spam being sent across the Internet, and the security issues raised because spam can be used to disrupt service or as a vehicle for sending viruses.

In particular, deceptive spam is an ever-growing problem that the FTC is addressing through law enforcement efforts, consumer and business education, and research. An important tool the FTC uses to target law violations, identify trends, and conduct research for education is its spam database. Consumers forward spam they receive to the FTC database at *uce@ftc.gov.* The database receives, on average, more than 110,000 e-mail messages each day, and currently contains a total of approximately 42 million pieces of spam.

In April 2003, the FTC released a report analyzing false claims made in spam. To prepare the report, the FTC staff reviewed a sample of approximately 1,000 pieces of spam, taken from a pool of more than 11 million e-mails in the FTC's database. Of the 1,000 pieces, 66 percent contained facial elements of deception in the "from" line, the "subject" line, or the text of the message.[17]

The FTC shares the database information with other Federal and state law enforcement agencies to broaden the fight against deceptive spam. In November 2002, the FTC and 12 law enforcement partners brought 30 enforcement actions as part of an ongoing initiative to fight deceptive spam and Internet scams.[18] The FTC also announced, with ten participating agencies, a "Spam Harvest," a study designed to

[12] FTC Facts for Businesses, *Financial Institutions and Customer Data: Complying with the Safeguards Rule,* available at <*http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm* >.

[13] 15 U.S.C. §§ 6501–6506.

[14] *United States* v. *Hershey Foods Corp.,* Civ. Action No. 4:03–cv–00350–JEJ (M.D. Pa. Feb. 26, 2003); *United States* v. *Mrs. Fields Famous Brands,* Civ. Action No. 2:03cv00205 (D. Utah Feb. 25, 2003); *United States* v. *The Ohio Art Co.,* Civ. Action No. 3:02CV7203 (N.D. Ohio Apr. 30, 2002); *United States* v. *American Pop Corn Co.,* Civ. Action No. C02–4008DEO (N.D. Iowa Feb. 28, 2002); *United States* v. *Lisa Frank, Inc.,* Civ. Action No. 01–1516–A (E.D. Va. Oct. 3, 2001); *United States* v. *Looksmart, Ltd.,* Civ. Action No. 01–606–A (E.D. Va. Apr. 23, 2001); *United States* v. *Bigmailbox.com, Inc.,* Civ. Action No. 01–605–A (E.D. Va. Apr. 23, 2001); *United States* v. *Monarch Servs., Inc.,* Civ. Action No. AMD 01 CV 1165 (D. Md. Apr. 20, 2001).

[15] *United States* v. *Hershey Foods Corp.,* Civ. Action No. 4:03-cv-00350–JEJ (M.D. Pa. Feb. 26, 2003); *United States* v. *Mrs. Fields Famous Brands,* Civ. Action No. 2:03cv00205 (D. Utah Feb. 25, 2003).

[16] Unsolicited commercial e-mail ("UCE" or "spam") is any commercial e-mail message that is sent—typically in bulk—to consumers without the consumers' prior request or consent.

[17] FTC STAFF REPORT, FALSE CLAIMS IN SPAM (Apr. 2003), available at <*http://www.ftc.gov/reports/spam/030429spamreport.pdf*>. The remaining spam messages were not necessarily truthful, but they did not contain any obvious indicia of falsity.

[18] FTC Press Release, *Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams* (Nov. 13, 2002), available at <*http://www.ftc.gov/opa/2002/11/netforce.htm*>.

identify online actions that may put consumers at the greatest risk for receiving spam.[19]

The FTC recently settled an action against a company that allegedly profited from a particularly insidious spam scam. According to the complaint, the subject line of the e-mail said "Yahoo sweepstakes winner," and the message congratulated the recipient for being chosen as a winner of a prize in a recent Yahoo sweepstakes contest. Most often, the message mentioned that the prize was a Sony Playstation 2, making it particularly attractive to adolescents. But the message was not from Yahoo, and the recipients had not won anything. Instead, after clicking through five web pages, consumers were connected to a pornographic website at a cost of up to $3.00 a minute. The settlement enjoins the defendants from making misleading representations of material facts in e-mail and other marketing, including deceptive e-mail header information. The settlement also requires the defendants to prevent third parties that promote their videotext services, through e-mail or other means, from making deceptive statements.[20]

In April, the FTC filed an action against an allegedly illegal spam operation for using false return addresses, empty "reply-to" links, and deceptive subject lines to expose unsuspecting consumers, including children, to sexually explicit material.[21] The FTC alleged that the defendant used the spam in an attempt to drive business to an adult website, "Married But Lonely." The FTC obtained a stipulated preliminary injunction to halt false or misleading spam.

The FTC recently hosted a three-day public forum to analyze the impact spam has on consumers' use of e-mail, e-mail marketing, and the Internet industry and to explore solutions in addition to law enforcement.[22] A major concern expressed at the forum was the dramatic rate at which spam is proliferating. For example, one ISP reported that in 2002, it experienced a 150 percent increase in spam traffic. America Online reported that it recently blocked 2.37 billion pieces of spam in a single day. Indeed, spam appears to be the marketing vehicle of choice for many fraudulent and deceptive marketers. In addition, and of particular concern, panelists noted that spam is increasingly used to disseminate malicious code such as viruses and "Trojan horses."

Solutions to the problems posed by spam will not be quick or easy; nor is one single approach likely to provide a cure. Instead, a balanced blend of technological fixes, business and consumer education, legislation, and enforcement will be required. Technology that empowers consumers in an easy-to-use manner is essential to getting immediate results for a number of frustrated end-users. Any solution to the problems caused by spam should contain the following elements:

1. Enhanced enforcement tools to combat fraud and deception;
2. Support for the development and deployment of technological tools to fight spam;
3. Enhanced business and consumer education; and
4. The study of business methods to reduce the volume of spam.

The Commission's legislative recommendations, outlined in Part IV, would enhance the agency's enforcement tools for fighting spam. In addition, the FTC will continue vigorous law enforcement and reach out to key law enforcement partners through the creation of a Federal/State Spam Task Force to strengthen cooperation with criminal authorities. The Task Force can help to overcome some of the obstacles that spam prosecutions present to law enforcement authorities. For example, in some instances, state agencies spent considerable front-end investigative resources to find a spammer, only to discover at the back end that the spammer was located outside the state's jurisdiction. State and Federal agencies recognize the need to share the information obtained in investigations, so that the agency best placed to pursue the spammer can do so more efficiently and quickly. The Task Force should facilitate this process. Further, it can serve as a forum to apprise participating agencies of the latest spamming technology, spammer ploys, and investigational techniques.

Through the Task Force, the FTC will reach out not only to its civil law enforcement counterparts on the state level, but also to Federal and state criminal authori-

[19] *See* FTC Consumer Alert, *E-mail Address Harvesting: How Spammers Reap What You Sow* (Nov. 13, 2002), available at <*http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm*>.

[20] *FTC* v. *BTV Indus.,* Civ. Action No. CV–S–02–0437–LRH–PAL (D. Nev. Jan. 6, 2003).

[21] *FTC* v. *Brian D. Westby,* Civ. Action No. 03–C–2540 (N.D. Ill. filed Apr. 15, 2003).

[22] Draft transcripts of the forum are available at <*http://www.ftc.gov/bcp/workshops/spam/index.html*>.

ties. Although few criminal prosecutions involving spam have occurred to date,[23] criminal prosecution may well be appropriate for the most egregious conduct. The FTC and its partners in criminal law enforcement agencies continue to work to assess existing barriers to successful criminal prosecutions. The FTC will explore whether increased coordination and cooperation with criminal authorities would be helpful in stopping the worst actors.

Improved technological tools will be an essential part of any solution as well. A great deal of spam is virtually untraceable, and an increasing amount crosses international boundaries. Panelists estimated that from 50 percent to 90 percent of e-mail is untraceable, either because it contains falsified routing information or because it comes through open relays or open proxies.[24] Because so much spam is untraceable, technological development will be an important element in solving spam problems. To this end, the FTC will continue to encourage industry to meet this challenge.

Action by consumers and businesses who may receive spam will be a crucial part of any solution to the problems caused by spam. A key component of the FTC's efforts against spam is educating consumers and businesses about the steps they can take to decrease the amount of spam they receive. The FTC's educational materials provide guidance on how to decrease the chances of having an e-mail address harvested and used for spam, and suggest several other steps to decrease the amount of spam an address may receive. The FTC's educational materials on spam are available on the FTC website.[25]

Finally, several initiatives for reducing the overwhelming volume of spam were discussed at the FTC's Spam Forum. At this point, questions remain about the feasibility and likely effectiveness of these initiatives. The FTC intends to continue its active role as catalyst and monitor of technological innovation and business approaches to addressing spam.

6. Pretexting. Through its Section 5 authority as well as its jurisdiction under the GLB Act, the FTC is also combating "pretexting," the use of false pretenses to obtain customer financial information. The agency has obtained stipulated court orders to halt these practices[26] and has sent warning letters to nearly 200 others about apparent violations of the GLB pretexting prohibitions.

C. Deceptive Lending Practices

As highlighted above, the FTC has been aggressive in its fight against deceptive lending practices. Unscrupulous lenders can deceive consumers about loan terms, rates, and fees, and the resulting injury can be severe—including the loss of a home. Over the last year, the FTC has obtained settlements for nearly $300 million in consumer redress for deceptive lending practices and other related law violations. The FTC has settled cases against Associates First Capital Corporation (now owned by

---

[23] *See, e.g., United States* v. *Barrero,* Crim. No. 03–30102–01 DRH (S.D. Ill. 2003) (guilty plea entered May 12, 2003). Like the related case, *FTC* v. *Stuffingforcash.com Corp.,* Civ. Action No. 02 C 5022 (N.D. Ill. Jan. 30, 2003), the allegations in this criminal prosecution were based on fraud in the seller's underlying business transaction.

[24] An open relay is an e-mail server that is configured to accept and transfer e-mail on behalf of any user anywhere, including unrelated third parties, which allows spammers to route their e-mail through servers of other organizations, disguising the origin of the e-mail. An open proxy is a mis-configured proxy server through which an unauthorized user can connect to the Internet. Spammers use open proxies to send spam from the computer network's ISP or to find an open relay.

Brightmail recently estimated that 90 percent of the e-mail that it analyzed was untraceable. Two panelists at the forum estimated that 40 percent to 50 percent of the e-mail it analyzed came through open relays or open proxies, making it virtually impossible to trace. Even when spam cannot be traced technologically, however, enforcement is possible. In some cases, the FTC has followed the money trail to pursue sellers who use spam. The process is resource intensive, frequently requiring a series of ten or more CIDs to identify and locate the seller in the real world. Frequently the seller and the spammer are different entities. In numerous instances, FTC staff cannot initially identify or locate the spammer and can only identify and locate the seller. In many of those cases, in the course of prosecuting the seller, staff has, through discovery, sought information about the spammer who actually sent the messages. This, too, involves resource-intensive discovery efforts. While the FTC actions have focused more on deception in the content of the spam *message,* recent actions have begun to attack deception in the *sending* of spam. As discussed above, the FTC has brought law enforcement actions targeting false subject lines and false "from" lines.

[25] *See <http://www.ftc.gov/spam>.*

[26] *FTC* v. *Information Search, Inc.,* Civ. Action No. AMD 01 1121 (D. Md. Mar. 15, 2002); *FTC* v. *Guzzetta,* Civ. Action No. CV–01–2335 (E.D.N.Y. Feb. 25, 2002); *FTC* v. *Garrett,* Civ. Action No. H 01–1255 (S.D. Tex. Mar. 25, 2003).

Citigroup)[27] for alleged deceptive sales of credit insurance and alleged violations of the Equal Credit Opportunity Act[28] and the Fair Credit Reporting Act;[29] against First Alliance Mortgage[30] for alleged deceptive loan terms and origination fees; and against Mercantile Mortgage[31] for alleged deception of consumers about loan terms and alleged violations of the Truth in Lending Act.[32] In addition to monetary relief, the Mercantile settlement gives hundreds of consumers the opportunity to refinance loans at low or no cost.[33]

D. Health Fraud and Deception

Truthful and substantiated advertising can serve as an important source of useful information for consumers about health care. Inaccurate information, on the other hand, can cause serious financial as well as physical harm. For that reason, combating deceptive health claims, both online and off, continues to be a priority for the FTC.

1. Dietary Supplements. Challenging misleading or unsubstantiated claims in the advertisement of dietary supplements is a significant part of the FTC's consumer protection agenda. During the past decade, the FTC has filed more than 80 law enforcement actions challenging false or unsubstantiated claims about the efficacy or safety of a wide variety of supplements.[34] The agency focuses its enforcement priorities on claims for products with unproven benefits or that present significant safety concerns to consumers, and on deceptive or unsubstantiated claims that products treat or cure serious diseases. The FTC has taken action against all parties responsible for the deceptive marketing, including manufacturers, advertising agencies, infomercial producers, distributors, retailers, and endorsers.

2. Weight Loss Advertising. Since the 1990s, the FTC has filed nearly 100 cases challenging false or misleading claims for all types of weight loss products, including over-the-counter drugs, dietary supplements, commercial weight loss centers, weight loss devices, and exercise equipment.[35] In September 2002, the FTC issued a "Report on Weight-Loss Advertising: An Analysis of Current Trends,"[36] which concludes that false or misleading claims for weight loss products are widespread and, despite an unprecedented level of FTC enforcement activity, appear to have increased over the last decade.

The FTC continues to explore ways to reduce the number of deceptive weight loss claims. On November 19, 2002, the FTC held a public workshop on the Advertising of Weight Loss Products.[37] Workshop participants included government officials, scientists, public health groups, marketers of weight loss products, advertising professionals, and representatives of the media. Participants explored both the impact of deceptive weight loss product ads on the public health and new approaches to fighting the proliferation of misleading claims, including a more active role for the media in screening out patently false weight loss advertising. Also, in an opinion piece in

---

[27] *FTC* v. *Associates First Capital Corp.,* Civ. Action No. 1:01–CV–00606 JTC (N.D. Ga. Feb. 26, 2002).

[28] 15 U.S.C. §§ 1691–1691f, *as amended.*

[29] *Id.* §§ 1681–1681(u), *as amended.*

[30] *FTC* v. *First Alliance Mortgage Co.,* Civ. Action No. SACV 00–964 DOC (MLGx) (C.D. Calif. Nov. 26, 2002).

[31] *U.S.* v. *Mercantile Mortgage Co.,* Civ. Action No. 02C 5079 (N.D. Ill. Aug. 15, 2002).

[32] 15 U.S.C. §§ 1601–1667f, *as amended.*

[33] The FTC continues its litigation against Chicago-area mortgage broker Mark Diamond and against D.C.-area mortgage lender Capital City Mortgage Corporation. *FTC* v. *Mark Diamond,* Civ. Action No. 02C–5078 (N.D.Ill. filed Nov. 1, 2002); *FTC* v. *Capital City Mortgage Corp.,* Civ. Action No. 1: 98–CV–00237 (D.D.C. Jan. 29, 1998). The *Diamond* case represents the FTC's first litigated case against a mortgage broker. In *Capital City,* the FTC alleges that Capital City deceived consumers into taking out high-rate, high-fee loans and then foreclosed on consumers' homes when they could not afford to pay.

[34] *See, e.g., FTC* v. *Dr. Clark Research Ass'n,* Civ. Action No. 1–03–00054–TRA (N.D. Ohio Jan. 8, 2003); *FTC v. Vital Dynamics,* Civ. Action No. 02–CV–9816 (C.D. Calif. Jan 17, 2003) (consent decree); *FTC* v. *Rexall Sundown, Inc.,* Civ. Action No. 00–CV–7016 (S.D. Fla. Mar. 11, 2003) (proposed consent decree subject to court approval).

[35] *See, e.g., Enforma Natural Prods., Inc.,* Civ. Action No. 2:00cv04376JSL (CWx) (C.D. Cal. Dec. 9, 2002) (consent decree); *Weider Nutrition Int'l,* Dkt. No. C–3983, 2001 WL 1717579 (Nov. 15, 2000); *FTC* v. *SlimAmerica, Inc.,* 77 F. Supp. 2d 1263 (S.D. Fla.1999); *Jenny Craig, Inc.,* 125 F.T.C. 333 (1998) (consent order); *Weight Watchers Int'l, Inc.,* 124 F.T.C. 610 (1997) (consent order); *NordicTrack, Inc.,* 121 F.T.C. 907 (1996) (consent order).

[36] FTC STAFF REPORT, WEIGHT LOSS ADVERTISING: AN ANALYSIS OF CURRENT TRENDS (Sept. 2002), available at <*http://www.ftc.gov/bcp/reports/weightloss.pdf*>.

[37] *See* Public Workshop: Advertising of Weight Loss Products, 67 Fed. Reg. 59,289 (Sept. 20, 2002).

Advertising Age, Commissioner Sheila Anthony noted that the FTC cannot solve this problem alone and challenged the industry and the media to play their part.[38]

E. Cross-Border Consumer Protection

The Internet and electronic commerce know no boundaries, and cross-border fraud is a growing problem for consumers and businesses in the U.S. and abroad. During 2002, approximately 14 percent of the complaints collected in the Consumer Sentinel complaint database involved a cross-border element. The number of FTC cases involving offshore defendants, offshore evidence, or offshore assets also has increased. In 2002, the FTC brought approximately 22 law enforcement actions involving cross-border fraud.

Those who defraud consumers take advantage of the special problems faced by law enforcers in acting against foreign companies, including difficulties in sharing information with foreign law enforcement agencies, exercising jurisdiction, and enforcing judgments abroad. Thus, law enforcers worldwide, now more than ever, need to cooperate and expand their consumer protection efforts.

To address the growing problem of cross-border fraud, in October 2002, Chairman Muris announced a Five-Point Plan to Combat Cross-Border Fraud. Since then, the FTC has been implementing this plan by:

- *Developing OECD guidelines on cross-border fraud.* Commissioner Mozelle Thompson of the FTC chairs the OECD Committee on Consumer Policy and leads the U.S. delegation to the Committee, which is developing guidelines for international cooperation concerning cross-border fraud. The FTC is working with its foreign counterparts, and soon expects to finalize these guidelines.
- *Strengthening bilateral and multilateral relationships.* The FTC already has bilateral consumer protection cooperation agreements with agencies in Australia, Canada, and the U.K., and is working to strengthen these relationships and develop new ones. The FTC also participates in a network of consumer protection enforcement officials from more than 30 countries. Finally, the FTC has joined other agencies in various cross-border task forces, such as the Toronto Strategic Partnership, Project Emptor with British Columbia authorities, and MUCH—the Mexico-U.S.-Canada Health fraud task force. In the past year, the FTC has announced numerous joint law enforcement actions taken with the assistance of these task forces, including actions involving credit card loss protection,[39] advance fee credit cards,[40] and bogus cancer clinics.[41]
- *Continuing public-private partnerships.* The FTC continues to ask responsible industry to help fight cross-border fraud, which hurts businesses as well as consumers. The FTC held a workshop on this issue in February 2003 and continues to work with the private sector to follow up on some ideas discussed at the workshop, including better sharing of information between the private sector and the FTC.
- *Providing technical assistance.* The FTC wants to ensure that no developing country becomes a haven for fraud. Therefore, it is conducting U.S. AID-funded technical assistance on consumer protection issues in various developing countries. Last year, the FTC conducted technical assistance missions for consumer protection authorities from 13 Eastern European countries, including Hungary and Slovenia. This year, the FTC is planning to conduct missions in Romania, Russia, and Peru.
- *Recommending proposals for legislative amendments.* Many of the challenges the FTC faces in combating cross-border fraud might best be addressed through legislative changes. The FTC's proposals for legislative changes are described in Section IV of this testimony.

F. Initiatives Designed to Reach Specific Consumer Groups

The FTC has implemented a variety of initiatives that assist particular consumer groups, including children, Spanish-speaking consumers, and military personnel and their families.

1. Protecting Children. The agency maintains an active program to monitor, report on, and provide educational materials about marketing activities affecting children. The FTC continues to monitor the marketing of violent entertainment products to children. Since September 2000, the agency has issued a series of reports on this

[38] Commissioner Sheila Anthony, *Let's clean up the diet-ad mess,* ADVERTISING AGE, Feb. 3, 2003, at 18.
[39] *FTC* v. *STF Group,* Civ. Action No. 03–C–0977 (N.D. Ill. filed Feb. 10, 2003).
[40] *FTC* v. *Pacific First Benefit,* LLC, Civ. Action No. 02–C–8678 (N.D. Ill. filed Dec. 2, 2003).
[41] *FTC* v. *CSCT, Inc.,* Civ. Action No. 03–C–00880 (N.D. Ill. filed Feb. 6, 2003).

issue.[42] The FTC intends to issue a fourth follow-up report on the industries' practices. The staff also is working with retailer trade groups to devise a consumer education message for parents, and is preparing to hold a public workshop on these issues later this year.

The FTC also conducted an informal survey of online gambling sites and published a consumer alert warning parents and their children that online gambling can pose huge risks, including money loss, impaired credit ratings, and addiction to gambling.[43]

Finally, the FTC monitors alcohol advertising to ensure that ads for these products do not involve potentially unfair or deceptive practices, including the targeting of alcohol advertisements to minors. In response to a Congressional request, the agency will prepare reports on two subjects related to alcohol advertising and youth: (1) the impact on underage consumers of the significant expansion of ads for new alcoholic beverages, and (2) the industry's response to recommendations for improved self-regulation contained in the FTC's 1999 report to Congress.[44]

2. Spanish-Speaking Consumers. In FY 2002, the FTC instituted a Hispanic Outreach Program, which resulted in hiring a Hispanic Outreach Coordinator. This effort includes the creation of a dedicated page on the FTC site, *Protection Para el Consumidor* ("Consumer Protection"), which mirrors the English version of the consumer protection page and provides Spanish translations of several popular consumer education publications. The FTC also has created an online Spanish-language consumer complaint form and has undertaken outreach efforts to Hispanic media.

In addition, the FTC has taken action against alleged law violations affecting Spanish-speaking consumers. The agency settled a civil penalty action against a Houston-based debt collection company for alleged violations of the rights of Spanish-and English-speaking consumers under the Fair Debt Collection Practices Act.[45] The settlement requires, among other things, that the company make disclosures in Spanish where applicable.

3. Military Sentinel. In September 2002, the FTC and the Department of Defense ("DOD") launched Military Sentinel, the first online consumer complaint database tailored to the unique needs of the military community. The system offers members of the military and their families a way to file complaints and gain immediate access to the FTC's full range of educational materials and information.[46] It also gives DOD and law enforcement officers secure access to the complaints entered into the database.

III. Maintaining Competition

The FTC's competition mission, as its name suggests, promotes competition in the marketplace to give consumers the best products at the lowest prices. The FTC employs a variety of tools to promote and protect competition: in addition to enforcing the antitrust laws, the agency holds workshops, conducts studies, writes reports, and monitors the marketplace. The agency will continue to focus both its law enforcement activity and other initiatives in key sectors of the economy, such as health care, energy, and high-tech industries. The global economy also requires the FTC's competition mission, like its consumer protection mission, to be increasingly concerned with international issues.

---

[42] FTC, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A REVIEW OF SELF-REGULATION AND INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (Sept. 2000), available at *<http://www.ftc.gov/reports/violence/vioreport.pdf>*; FTC, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A SIX-MONTH FOLLOW-UP REVIEW OF INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (Apr. 2001), available at *<http://www.ftc.gov/reports/violence/violence010423.pdf>*;

FTC, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A ONE-YEAR FOLLOW-UP REVIEW OF INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (Dec. 2001), available at *<http://www.ftc.gov/os/2001/12/violencereport1.pdf>*;

FTC, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A TWENTY-ONE MONTH FOLLOW-UP REVIEW OF INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (June 2002), available at *<http://www.ftc.gov/reports/violence/mvecrpt0206.pdf>*.

[43] FTC Consumer Alert, *Online Gambling and Kids: A Bad Bet* (June 26, 2002), available at *<http://www.ftc.gov/bcp/conline/pubs/alerts/olgamble.htm>*.

[44] Conference Report on the Omnibus Appropriations Bill for FY 2003, H. REP. NO. 108–10 (Feb. 13, 2003)

[45] *United States* v. *United Recovery Systems, Inc.,* Civ. Action No. H–02–1410 (sl) (S.D. Tex. Apr. 22, 2002).

[46] FTC Facts for Consumers, *Military Sentinel: Fact Sheet,* available at *<http://www.ftc.gov/bcp/conline/pubs/general/milsent_fact.htm>*.

A. Health Care

The health care sector remains enormously important to both consumers and the national economy. Health-related products and services account for more than 15 percent of the U.S. gross domestic product ("GDP"), and that share has grown by about 25 percent since 1990. Without effective antitrust enforcement, health costs would be greater and the share of GDP would be even higher.

1. Prescription Drugs. As previously mentioned, the FTC recently reached a major settlement with Bristol-Myers Squibb ("BMS") to resolve charges that BMS engaged in a series of anticompetitive acts over the past decade to obstruct entry of low-price generic competition for three of BMS's widely-used pharmaceutical products: two anti-cancer drugs, Taxol and Platinol, and the anti-anxiety agent BuSpar.[47] Among other things, the FTC's complaint alleged that BMS abused FDA regulations to obstruct generic competitors; misled the FDA about the scope, validity, and enforceability of patents to secure listing in the FDA's "Orange Book" list of approved drugs and their related patents; breached its duty of good faith and candor with the U.S. Patent and Trademark Office ("PTO"), while pursuing new patents claiming these drugs; filed baseless patent infringement suits against generic drug firms that sought FDA approval to market lower-priced drugs; and paid a would-be generic rival $72.5 million to abandon its legal challenge to the validity of a BMS patent and to stay out of the market until the patent expired. Because of BMS's alleged pattern of anticompetitive conduct and the extensive resulting consumer harm, the Commission's proposed order necessarily contains strong—and in some respects unprecedented—relief.[48]

The settlement with BMS represents the latest FTC milestone in settlements regarding allegedly anticompetitive conduct by branded or generic drug manufacturers designed to delay generic entry. Other recent FTC successes in this area include:

- *Biovail.* An October 2002 consent order settling charges that Biovail Corporation illegally acquired a license to a patent and improperly listed the patent in the FDA's Orange Book as claiming Biovail's high blood pressure drug Tiazac (under current law, the listing of the patent and the subsequent lawsuit brought by Biovail against a potential generic entrant triggered an automatic 30-month stay of FDA approval of the generic competitor);[49] and
- *Biovail/Elan.* An August 2002 settlement with Biovail and Elan Corporation, plc resolving charges that the companies entered into an agreement that provided substantial incentives for the two companies not to compete in the markets for 30 milligram and 60 milligram dosage strengths of the generic drug Adalat CC (an anti-hypertension drug).[50]

2. Health Care Providers. For decades, the FTC has worked to facilitate innovative and efficient arrangements for the delivery and financing of health care services by challenging artificial barriers to competition among health care providers. These efforts continue. In the last year, the FTC settled with seven groups of physicians for allegedly colluding to raise consumers' costs.[51] These settlements involved significant numbers of doctors—more than 1,200 in a case in the Dallas-Fort Worth area and more than three-quarters of all doctors in the Carlsbad, New Mexico area. The Commission's orders put a stop to allegedly collusive conduct that harms employers, individual patients, and health plans by depriving them of the benefits of competition in the purchase of physician services.

3. Health Care Mergers. The FTC has taken action regarding a number of proposed mergers in the health care sector to ensure that consumers continue to receive the benefits of competitive markets. In April, the Commission reached a settlement with Pfizer Inc., the largest pharmaceutical company in the United States, and Pharmacia Corporation to resolve concerns that their $60 billion merger would harm competition in nine separate and wide-ranging product markets, including drugs to treat overactive bladder, symptoms of menopause, skin conditions, coughs,

---

[47] *Bristol-Myers Squibb Co.,* Dkt. No. C–4076 (Apr. 14, 2003).

[48] The proposed order includes a provision prohibiting BMS from triggering a 30-month stay for any BMS product based on any patent BMS lists in the Orange Book after the filing of an application to market a generic drug.

[49] *Biovail Corp.,* Dkt. No. C–4060 (Oct. 2, 2002).

[50] *Biovail Corp. and Elan Corp.,* Dkt. No. C–4057 (Aug. 15, 2002).

[51] *Grossmont Anesthesia Servs. Med. Group, Inc.,* File No. 021–0006 (May 30, 2003) (agreement accepted for public comment); *Anesthesia Serv. Med. Group, Inc.,* File No. 021–0006 (May 30, 2003) (agreement accepted for public comment); *Carlsbad Physicians,* File No. 031–0002 (May 2, 2003) (agreement accepted for public comment); *System Health Providers,* Dkt. No. C–4064 (Oct. 24, 2002); *R.T. Welter & Assoc., Inc.* (Professionals in Women's Care), Dkt. No. C–4063 (Oct. 8, 2002); *Physician Integrated Servs. of Denver, Inc.,* Dkt. No. C–4054 (July 16, 2002); *Aurora Associated Primary Care Physicians, L.L.C.,* Dkt. No. C–4055 (July 16, 2002).

motion sickness, erectile dysfunction, and three different veterinary conditions.[52] Annual sales in the nine product markets currently total more than $3 billion. The settlement will require divestitures to protect consumers' interests in those markets while allowing the remainder of the transaction to go forward.

Other recent health care mergers investigated by the FTC include:

- *Cytyc/Digene.* In June 2002, the Commission authorized the staff to seek a preliminary injunction blocking Cytyc Corporation's proposed acquisition of Digene Corporation,[53] involving the merger of two manufacturers of complementary cervical cancer screening tests. The complaint alleged that the combined firm would have an incentive to use its market power in one product to stifle increased competition in the complementary product's market. Thus, if the merger had been consummated, rivals would have been substantially impeded from competing. Following the Commission's decision, the parties abandoned the transaction.
- *Baxter/Wyeth.* The FTC alleged that Baxter International's $316 million acquisition of Wyeth Corporation raised competitive concerns in markets for a variety of drugs. Of particular concern were the $400 million market for propofol, a general anesthetic commonly used for the induction and maintenance of anesthesia during surgery, and the $225 million market for new injectable iron replacement therapies used to treat iron deficiency in patients undergoing hemodialysis.[54] To settle this matter, the parties agreed to divestitures that are expected to maintain competition in those markets.
- *Amgen/Immunex.* The FTC obtained an agreement settling allegations that Amgen Inc.'s $16 billion acquisition of Immunex Corporation would reduce competition for three important biopharmaceutical products: (1) neutrophil regeneration factors used to treat a dangerously low white blood cell count that often results from chemotherapy; (2) tumor necrosis factors used to treat rheumatoid arthritis, Crohn's disease, and psoriatic arthritis; and (3) interleukin-1 inhibitors used in the treatment of rheumatoid arthritis.[55] The settlement required that the companies divest certain assets and license certain intellectual property rights in these markets.

4. Promoting Competition in Prescription Drugs. The FTC also has sought to promote competition in the pharmaceutical industry through published reports and speeches. Commissioner Leary has a special interest in pharmaceutical competition and has addressed this topic in speeches to solicit input from affected parties and to promote dialogue regarding practical solutions.[56]

In July 2002, the FTC issued a report entitled "Generic Drug Entry Prior to Patent Expiration: An FTC Study,"[57] which evaluated whether the Hatch-Waxman Amendments to the Federal Food, Drug, and Cosmetic Act are susceptible to strategies to delay or deter consumer access to generic alternatives to brand-name drug products. The report recommended changes in the law to ensure that generic entry is not delayed unreasonably, including through anticompetitive activity. In October 2002, President Bush directed the FDA to implement one of the key findings identified in the FTC study.[58] Specifically, the FDA has proposed a new rule to curb one of the abuses uncovered by the FTC study—pharmaceutical firms' alleged misuse of the Hatch-Waxman patent listing provisions—to speed consumer access to lower-cost generic drugs.[59]

---

[52] *Pfizer Inc.,* Dkt. No. C–4075 (Apr. 14, 2003) (proposed consent agreement accepted for public comment).

[53] FTC Press Release, *FTC Seeks to Block Cytyc Corp.'s Acquisition of Digene Corp.* (June 24, 2002), available at <*http://www.ftc.gov/opa/2002/06/cytyc_digene.htm*>.

[54] *Baxter International Inc. and Wyeth,* Dkt. No. C–4068 (Feb. 3, 2003).

[55] *Amgen Inc. and Immunex Corp.,* Dkt. No. C–4056 (Sept. 3, 2002).

[56] *See* Thomas B. Leary, *Antitrust Issues in Settlement of Pharmaceutical Patent Disputes* (Nov. 3, 2000), available at <*http://www.ftc.gov/speeches/leary/learypharma.htm*>; Thomas B. Leary, *Antitrust Issues in the Settlement of Pharmaceutical Patent Disputes, Part II* (May 17, 2001), available at <*http://www.ftc.gov/speeches/leary/learypharmaceutical settlement.htm*>.

[57] GENERIC DRUG ENTRY PRIOR TO PATENT EXPIRATION: AN FTC STUDY (July 2002), available at <*http://www.ftc.gov/opa/2002/07/genericdrugstudy.htm*>.

[58] President Takes Action to Lower Prescription Drug Prices by Improving Access to Generic Drugs (Oct. 21, 2002), available at <*http://www.whitehouse.gov/news/releases/2002/10/20021021–2.html*>.

[59] Applications for FDA Approval to Market a New Drug: Patent Listing Requirements and Application of 30-Month Stays on Approval of Abbreviated New Drug Applications Certifying That a Patent Claiming a Drug Is Invalid or Will Not Be Infringed; Proposed Rule, 67 Fed. Reg. 65448 (Oct. 24, 2002).

5. Hearings on Health Care and Competition Law and Policy. To keep abreast of developments in the dynamic health care market, the FTC, working with DOJ's Antitrust Division, commenced a series of hearings on "Health Care and Competition Law and Policy" on February 26, 2003.[60] Over a seven-month period, the FTC and DOJ will spend almost 30 days of hearings in a comprehensive examination of a wide range of health care issues, involving hospitals, physicians, insurers, pharmaceuticals, long-term care, Medicare, and consumer information, among others. To date, the hearings have focused on the specific challenges and complications involved in applying competition law and policy to health care; issues involved in hospital merger cases and other joint arrangements, including geographic and product market definition; horizontal hospital networks and vertical arrangements with other health care providers; the competitive effects of mergers of health insurance providers; and consumer information and quality of care issues. A public report that incorporates the results of the hearings will be prepared after the hearings.

B. Energy

Antitrust law enforcement is critical in the oil and gas industry. Fuel price increases directly and significantly affect businesses of all sizes throughout the U.S. economy and can strain consumer budgets.

1. Oil Merger Investigations. In recent years, the FTC has investigated numerous oil mergers. When necessary, the agency has insisted on divestitures to cure potential harm to competition. In the most recent case, *Conoco/Phillips,* the Commission required the merged company to divest two refineries and related marketing assets, terminal facilities for light petroleum and propane products, and certain natural gas gathering assets.[61]

2. Natural Gas Merger Investigations. The FTC also has investigated mergers in the natural gas industry and taken necessary action to preserve competition. Just two weeks ago, the Commission accepted for public comment a consent order designed to preserve competition in the market for the delivery of natural gas to the Kansas City area.[62] The proposed order conditionally would allow Southern Union Company's $1.8 billion purchase of the Panhandle pipeline from CMS Energy Corporation, while requiring Southern Union to terminate an agreement under which one of its subsidiaries managed the Central pipeline, which competes with Panhandle in the market for delivery of natural gas to the Kansas City area. Absent the settlement agreement, the transaction would have placed the two pipelines under common ownership or common management and control, eliminating direct competition between them, and likely resulting in consumers' paying higher prices for natural gas in the Kansas City area.

3. Gasoline Monopolization Case. As highlighted above, the Commission recently issued an administrative complaint in an important nonmerger case involving the Union Oil Company of California ("Unocal").[63] The complaint alleges that Unocal violated Section 5 of the FTC Act by subverting the California Air Resources Board's ("CARB") regulatory standard-setting procedures of the late 1980s relating to low-emissions reformulated gasoline ("RFG"). According to the complaint, Unocal misrepresented to industry participants that some of its emissions research was non-proprietary and in the public domain, while at the same time pursuing a patent that would permit Unocal to charge royalties if CARB used such emissions information. The complaint alleged that Unocal did not disclose its pending patent claims and that it intentionally perpetuated the false and misleading impression that it would not enforce any proprietary interests in its emissions research results. The complaint states that Unocal's conduct has allowed it to acquire monopoly power for the technology to produce and supply California "summer-time" RFG, a low-emissions fuel mandated for sale in California from March through October, and could cost California consumers five cents per gallon in higher gasoline prices. This case is pending before an Administrative Law Judge.

4. Study of Refined Petroleum Product Prices. Building on its enforcement experience in the petroleum industry, the FTC is studying the causes of volatility in refined petroleum products prices. In two public conferences, held in August 2001 and

---

[60] The FTC website for the hearings is *http://www.ftc.gov/ogc/healthcarehearings/index.htm.* To date, the FTC has released a detailed agenda for the hearings' sessions in February through June. All of the documents relating to the hearings appear on the website.

[61] *Conoco Inc. and Phillips Petroleum Company,* Dkt. No. C–4058 (Feb. 7, 2003) (consent order).

[62] *Southern Union Co.,* File No. 031–0068 (May 29, 2003) (agreement accepted for public comment).

[63] *Union Oil Co. of California,* Dkt. No. 9305 (complaint issued Mar. 4, 2003).

May 2002,[64] participants discussed key factors that affect product prices, including increased dependency on foreign crude sources, changes in industry business practices, and new governmental regulations. The information gathered through these public conferences will form the basis for a report to be issued later this year.

5. Gasoline Price Monitoring. In May 2002, the FTC announced a project to monitor wholesale and retail prices of gasoline in an effort to identify possible anticompetitive activities to determine if a law enforcement investigation would be warranted. This project tracks retail gasoline prices in approximately 360 cities nationwide and wholesale (terminal rack) prices in 20 major urban areas. The FTC Bureau of Economics staff receives daily data purchased from the Oil Price Information Service ("OPIS"), a private data collection company. The economics staff uses an econometric (statistical) model to determine whether current retail and wholesale prices each week are anomalous in comparison with historical data. This model relies on current and historical price relationships across cities, as well as other variables.

As a complement to the analysis based on OPIS data, the FTC staff also regularly reviews reports from the Department of Energy's Consumer Gasoline Price Hotline, searching for prices significantly above the levels indicated by the FTC's econometric model or other indications of potential problems. Throughout most of the past two years, gasoline prices in U.S. markets have been within their predicted normal bounds. Of course, the major factor affecting U.S. gasoline prices is the substantial fluctuation in crude oil prices. Prices outside the normal bounds trigger further staff inquiry to determine what factors might be causing price anomalies in a given area. These factors could include supply disruptions such as refinery or pipeline outages, changes in taxes or fuel specifications, unusual changes in demand due to weather conditions and the like, and possible anticompetitive activity.

To enhance the Gasoline Price Monitoring Project, the FTC has recently asked each state Attorney General to forward to the FTC's attention consumer complaints they receive about gasoline prices. The staff will incorporate these complaints into its ongoing analysis of gasoline prices around the country, using the complaints to help locate price anomalies outside of the 360 cities for which the staff already receives daily pricing data.

The goal of the Monitoring Project is to alert the FTC to unusual changes in gasoline prices so that further inquiry can be undertaken expeditiously. When price increases do not appear to have market-driven causes, the FTC staff will consult with the Energy Information Agency of the Department of Energy. The FTC staff also will contact the offices of the appropriate state Attorneys General to discuss the anomaly and the appropriate course for any further inquiry, including the possible opening of a law enforcement investigation.

C. High Technology

With its history of keeping pace with marketplace developments, the FTC is well-positioned to take a leading role in assessing the impact of technology on domestic and world markets. In addition to bringing enforcement actions in high tech areas, the FTC is studying the impact of the Internet and intellectual property on competition law and policy.

1. Standard-Setting Cases. As technology advances, efforts will increase to establish industry standards for the development and manufacture of new products. Standard setting is often procompetitive, but anticompetitive abuses can take place during the standard-setting process. When the standard-setting process appears to have been subverted, the FTC will take action. In addition to *Unocal,* discussed previously, the agency is currently conducting an administrative adjudication regarding Rambus, Inc. A June 2002 complaint alleges that Rambus, a participant in an electronics standard-setting organization, failed to disclose—in violation of the organization's rules—that it had a patent and several pending patent applications on technologies that eventually were adopted as part of the industry standard.[65] The standard at issue involved a common form of computer memory used in a wide variety of popular consumer electronic products, such as personal computers, fax machines, video games, and personal digital assistants. The Commission's complaint alleges that, once the standard was adopted, Rambus was in a position to reap millions in royalty fees each year, and potentially more than a billion dollars over the life of

[64] FTC Press Release, *FTC to Hold Public Conference/Opportunity for Comment on U.S. Gasoline Industry in Early August* (July 12, 2001), available at *<http://www.ftc.gov/opa/2001/07/gasconf.htm>*; FTC Press Release, *FTC Chairman Opens Public Conference Citing New Model To Identify and Track Gasoline Price Spikes, Upcoming Reports* (May 8, 2002), available at *<http://www.ftc.gov/opa/2002/05/gcr.htm>*.

[65] *Rambus, Inc.,* Dkt. No. 9302 (complaint issued June 18, 2002).

the patents.[66] Because standard-setting abuses can harm robust and efficiency-enhancing competition in high tech markets, the FTC will continue to pursue investigations in this area.[67]

2. Intellectual Property Hearings. In 2002, the FTC and DOJ commenced a series of ground-breaking hearings on "Competition and Intellectual Property Law and Policy in the Knowledge-Based Economy."[68] These hearings, which took place throughout 2002 and were held in Washington and Silicon Valley, heard testimony from academics, industry leaders, technologists and others about the increasing need to manage the issues at the intersection of competition and intellectual property law and policy. The FTC anticipates releasing a report on its findings later this year.

3. Internet Task Force. In 2001, the FTC's Internet Task Force began to evaluate potentially anticompetitive regulations and business practices that could impede e-commerce. The Task Force has discovered that some state regulations may have the effect of protecting existing bricks-and-mortar businesses from new Internet competitors. The Task Force also is considering whether private companies may be hindering e-commerce through the use of potentially anticompetitive tactics. In October 2002, the Task Force held a public workshop to: (1) enhance the FTC's understanding of these issues; (2) educate policymakers about the potential anticompetitive effects of state regulations; and (3) educate private entities about the types of business practices that may be viewed as problematic.[69]

D. International Competition

Because competition increasingly takes place in a worldwide market, cooperation with competition agencies in the world's major economies is a key component of the FTC's enforcement program. Given differences in laws, cultures, and priorities, it is unlikely that there will be complete convergence of antitrust policy in the foreseeable future. Areas of agreement far exceed those of divergence, however, and instances in which differences will result in conflicting results are likely to remain rare. The agency has increased its cooperation with agencies around the world, both on individual cases and on policy issues, and is committed to addressing and minimizing policy divergences.

1. ICN and ICPAC. In the fall of 2001, the FTC, DOJ, and 12 other antitrust agencies from around the world launched the International Competition Network ("ICN"), an outgrowth of a recommendation of the International Competition Policy Advisory Committee ("ICPAC"). ICPAC suggested that competition officials from developed and developing countries convene a forum in which to work together on competition issues raised by economic globalization and the proliferation of antitrust regimes. The ICN provides a venue for antitrust officials worldwide to work toward consensus on proposals for procedural and substantive convergence on best practices in antitrust enforcement and policy. Sixty-seven jurisdictions already have joined the ICN, and the FTC staff is working on initial projects relating to mergers and competition advocacy.

2. OECD. The FTC continues to participate in the work of the OECD on, among other things, merger process convergence, implementation of the OECD recommendation on hard-core cartels (*e.g.,* price-fixing agreements), and regulatory reform.

E. Other Enforcement

3. General Merger Enforcement. The FTC reviews and challenges mergers in any economic sectors that have significant potential to harm competition and consumers. For example, last summer the Commission settled allegations that Bayer AG's $6.2 billion purchase of Aventis S.A.'s crop science business raised antitrust concerns in the markets for a number of crop science products, including markets for (1) new generation chemical insecticide products and active ingredients; (2) post-emergent grass herbicides for spring wheat; and (3) cool weather cotton defoliants. These new generation products are at the forefront of pesticide, insecticide, and herbicide products, and maintaining competition in these markets is significant because they appear to offer greater effectiveness, with less environmental impact than current gen-

---

[66] *Id.*

[67] In 1996, the FTC settled a similar complaint against Dell Computer, alleging that Dell had failed to disclose an existing patent on a personal computer component that was adopted as the standard for a video electronics game. *Dell Computer Co.,* 121 F.T.C. 616 (1996).

[68] FTC Press Release, *Muris Announces Plans for Intellectual Property Hearings* (Nov. 15, 2001), available at <*http://www.ftc.gov/opa/2001/11/iprelease.htm*>.

[69] FTC Press Release, *FTC to Host Public Workshop to Explore Possible Anticompetitive Efforts to Restrict Competition on the Internet* (July 17, 2002), available at <*http://www.ftc.gov/opa/2002/07/ecom.htm*>.

eration products. In settling this matter, the Commission required Bayer to divest businesses and assets used in the manufacture of these products to parties capable of maintaining competitive conditions in these markets.[70]

Also, in October 2002, the Commission authorized the staff to seek a preliminary injunction in Federal court blocking the proposed acquisition of the Claussen Pickle Company by the owner of the Vlasic Pickle Company.[71] If allowed to proceed, the combined firm would have had a monopoly share of the refrigerated pickle market in the United States. Following the FTC's decision, the parties abandoned the proposed acquisition.

2. Mergers Not Reportable Under HSR. The FTC will continue to devote resources to monitoring merger activities that are not subject to premerger reporting requirements under HSR, but that could be anticompetitive. In 2000, Congress raised the HSR size-of-transaction filing threshold to eliminate the reporting requirement for smaller mergers, but of course it did not eliminate the substantive prohibition under Section 7 of the Clayton Act[72] against smaller mergers that may substantially lessen competition. Consequently, the FTC must identify—through means such as the trade press and other news articles, consumer and competitor complaints, hearings, and economic studies—and remedy those unreported, usually consummated mergers that could harm consumers.

One notable example is the case against MSC.Software Corporation.[73] In this case, the company ultimately agreed to settle FTC allegations that MSC's 1999 acquisitions of Universal Analytics, Inc. and Computerized Structural Analysis & Research Corporation violated Federal antitrust laws by eliminating competition in, and monopolizing the market for, advanced versions of Nastran, an engineering simulation software program used throughout the aerospace and automotive industries. Under the terms of the settlement agreement, MSC must divest at least one clone copy of its current advanced Nastran software, including the source code. The divestiture will be through royalty-free, perpetual, non-exclusive licenses to one or two acquirers who must be approved by the FTC.

3. Enforcement of FTC Merger Orders. The FTC also will litigate, when necessary, to ensure compliance with Commission orders protecting competition. In March, a Federal judge fined Boston Scientific Corporation ("BSC") for violating a licensing requirement in a merger settlement involving medical technology used to diagnose and treat heart disease.[74] To preserve competition in the market for intravascular ultrasound catheters following its acquisition of two competitors, BSC had agreed to license its catheter technology to Hewlett-Packard Company. Finding that BSC "acted in bad faith" and took an "obstreperous approach" to its obligation, the court assessed a civil penalty of more than $7 million. This represents the largest civil penalty ever imposed for violation of an FTC order.

IV. Legislative Recommendations

To improve the agency's ability to implement its mission and to serve consumers, the FTC makes the following recommendations for legislative changes. The FTC staff will be happy to work with Subcommittee staff on these recommendations.

A. Elimination of the FTC Act's Exemption for Communications Common Carriers

The FTC Act exempts common carriers subject to the Communications Act from its prohibitions on unfair or deceptive acts or practices and unfair methods of competition. This exemption dates from a period when telecommunications services were provided by government-authorized, highly regulated monopolies. The exemption is now outdated. In the current world, firms are expected to compete in providing telecommunications services. Congress and the Federal Communications Commission ("FCC") have replaced much of the economic regulatory apparatus formerly applicable to the industry with competition. Moreover, technological advances have blurred traditional boundaries between telecommunications, entertainment, and high technology. Telecommunications firms have expanded into numerous non-common-carrier activities. For these reasons, FTC jurisdiction over telecommunications firms' activities has become increasingly important.

The FTC Act exemption has proven to be a barrier to effective consumer protection, both in common carriage and in other telecommunications businesses. The exemption also has prevented the FTC from applying its legal, economic, and industry

[70] *Bayer AG and Aventis S.A.,* Dkt. No. C–4049 (July 24, 2002) (consent order).

[71] *FTC v. Hicks, Muse, Tate & Furst Equity Fund V, LP,* Civ. Action No. 1:02-cv-02070–RWR (D.D.C. filed Oct. 23, 2002). A notice of voluntary dismissal was filed on October 31, 2002.

[72] 15 U.S.C. § 18.

[73] *MSC.Software Corp.,* Dkt. No. 9299 (Oct. 29, 2002).

[74] *United States* v. *Boston Scientific Corp.,* Civ. Action No. 00–12247–PBS, Memorandum and Order (D. Mass. Mar. 28, 2003).

expertise regarding competition to mergers and other possible anticompetitive practices, not only involving common carriage but also in other high-tech fields involving telecommunications. The FTC believes that Congress should eliminate the special exemption to reflect the fact that competition and deregulation have replaced comprehensive economic regulation.

The common carrier exemption sometimes has stymied FTC efforts to halt fraudulent or deceptive practices by telecommunications firms. While common carriage has been outside the FTC's authority, the agency believes that the FTC Act applies to non-common-carrier activities of telecommunications firms, even if the firms also provide common carrier services. Continuing disputes over the breadth of the FTC Act's common carrier exemption hamper the FTC's oversight of the non-common-carrier activities. These disputes have arisen even when the FCC may not have jurisdiction over the non-common-carrier activity. These disputes may increase the costs of pursuing an enforcement action or may cause the agency to narrow an enforcement action—for example, by excluding some participants in a scheme—to avoid protracted jurisdictional battles and undue delay in providing consumer redress. It may have additional serious consequences to new areas of industry convergence, *e.g.,* high technology and entertainment, where the FTC's inability to protect consumers can undermine consumer confidence.

The FTC has the necessary expertise to address these issues. The FTC has broad consumer protection and competition experience covering nearly all fields of commerce. The FTC has extensive expertise with advertising, marketing, billing, and collection, areas in which significant problems have emerged in the telecommunications industry. In addition, the FTC has powerful procedural and remedial tools that could be used effectively to address developing problems in the telecommunications industry if the FTC were authorized to reach them.

The common carrier exemption also significantly restricts the FTC's ability to engage in effective antitrust enforcement in broad sectors of the economy. The mix of common carrier and non-common-carrier activities within particular telecommunications companies frequently precludes FTC antitrust enforcement for much of the telecommunications industry. Further, because of the expansion of telecommunications firms into other high-tech industries and the growing convergence of telecommunications and other technologies, the common carrier exemption increasingly limits FTC involvement in a number of industries outside telecommunications.

B. Legislation to Improve the FTC's Ability to Combat Cross-Border Fraud

As stated earlier, consumer fraud is now more global than ever before. To better protect consumers, the FTC requests that Congress enact legislation that would better address the changing nature of the consumer marketplace and improve the agency's ability to cooperate and share information in cases and investigations relating to cross-border fraud. The agency's recommendations focus primarily on improving its ability to combat fraud involving foreign parties, evidence, or assets. At the same time, some of the recommendations may also benefit the pursuit of purely domestic investigations and cases. Indeed, it is often not immediately evident whether a matter has a cross-border component.

These proposals also would help the FTC fight deceptive spam. As the agency has learned from investigations and discussions at the recent FTC spam forum, spammers easily can hide their identity, forge the electronic path of their e-mail messages, or send their messages from anywhere in the world to anyone in the world. Also, a large percentage of spam comes from outside our borders. For these reasons, the spam forum participants emphasized that successful efforts to combat deceptive spam will require international enforcement cooperation. These legislative proposals can improve the FTC's ability to cooperate with international partners on this issue.

The FTC staff has discussed these legislative proposals with other affected agencies, and these agencies generally support the goals of the proposals. The FTC staff is continuing to work with these agencies on the details of a few of the proposals.

The FTC's cross-border proposal includes four main components. First, the FTC is seeking to strengthen, in a number of ways, its ability to cooperate with foreign counterparts, who are often investigating the same targets. Under current law, for example, the FTC is prohibited from sharing with foreign counterparts certain information that the FTC has obtained in its investigations. Legislation is necessary to allow the agency to share such information and provide other investigative assistance in appropriate cases.[75]

[75] The Securities Exchange Commission, the Commodity Futures Trading Commission, and the Federal financial regulators already have the authority to share information and cooperate

Continued

Second, the FTC is seeking enhancements to its information-gathering capabilities to enable it to obtain more easily information from Federal financial regulators about those who may be defrauding consumers. The FTC is also seeking enhancement of its ability to obtain information from third parties without the request triggering advance notice to investigative targets and thus prompting the targets to move their assets overseas.

Third, the FTC is seeking improvements to its ability to obtain consumer redress in cross-border litigation, by clarifying the agency's authority to take action in cross-border cases and expanding its ability to use foreign counsel to pursue offshore assets.

Finally, the FTC is seeking to strengthen international cooperative relationships by obtaining authority to facilitate staff exchanges and to provide financial support for certain joint projects.

C. Legislation to Enhance the FTC's Effectiveness To Fight Fraudulent Spam

As discussed earlier, a recent study by the Commission found that 66 percent of spam contained obvious indicia of falsity. Moreover, a significant portion of spam is likely to be routed through foreign servers. For these reasons, it would be useful to have additional legislative authority, addressing both procedural and substantive issues, that would enhance the agency's effectiveness in fighting fraud and deception. The procedural legislative proposals would improve the FTC's ability to investigate possible spam targets, and the substantive legislative proposals would improve the agency's ability to sue these targets successfully.

1. Procedural Proposals. The FTC's law enforcement experience shows that the path from a fraudulent spammer to a consumer's in-box frequently crosses at least one international border and often several. Thus, fraudulent spam exemplifies the growing problem of cross-border fraud. Two of the provisions in the proposed cross-border fraud legislation discussed above also would be particularly helpful to enable the FTC to investigate deceptive spammers more effectively and work better with international law enforcement partners.

First, we request that the FTC Act be amended to allow FTC attorneys to seek a court order requiring a recipient of a Civil Investigative Demand ("CID") to maintain the confidentiality of the CID for a limited period of time. Several third parties have told us that they will provide notice to the target before they will share information with us, sometimes because they believe notice may be required and sometimes even if such notice clearly is not required by law.

Second, we are requesting that the FTC Act be amended to provide that FTC attorneys may apply for a court order temporarily delaying notice to an investigative target of a CID issued to a third party in specified circumstances, when the Right to Financial Privacy Act ("RFPA") or the Electronic Communications Privacy Act ("ECPA") would require such notice.

The FTC's experience is that when fraud targets are given notice of FTC investigations they often destroy documents or secrete assets. Currently RFPA and ECPA provide a mechanism for delaying notice, but the FTC's ability to investigate would be improved by tailoring the bases for a court-ordered delay more specifically to the types of difficulties the FTC encounters, such as transfers of assets offshore. In addition, it is unclear whether FTC attorneys can file such applications, or whether the Commission must seek the assistance of the Department of Justice. Explicit authority for the FTC, by its own attorneys, to file such applications would streamline the agency's investigations of purveyors of fraud on the Internet, ensuring that the agency can rapidly pursue investigative leads.

Other legislative proposals would enhance the FTC's ability to track deceptive spammers. First, we request that the ECPA be clarified to allow the FTC to obtain complaints received by an ISP regarding a subscriber. Frequently, spam recipients complain first to their ISPs, and access to the information in those complaints would help the agency to determine the nature and scope of the spammer's potential law violations, as well as lead the agency to potential witnesses.

Second, we request that the scope of the ECPA be clarified so that a hacker or a spammer who has hijacked a bona fide customer's e-mail account is deemed a mere unauthorized user of the account, not a "customer" entitled to the protections afforded by the statute. Because of the lack of a statutory definition for the term "customer," the current statutory language may cover hackers or spammers. Such a reading of the ECPA would permit the FTC to obtain only limited information

---

with their foreign counterparts. *See* 15 U.S.C. §78x(c); 15 U.S.C. §78u(a)(2); 7 U.S.C. §12(e); 7 U.S.C. §16(f); 12 U.S.C. §3109(a)-(b); and 12 U.S.C. §1818(v)(2). The FTC's proposal is modeled after these statutes.

about a hacker or spammer targeted in an investigation. Clarification to eliminate such a reading would be very helpful.

Third, we request that the ECPA be amended to include the term "discovery subpoena" in the language of 18 U.S.C. § 2703. This change is particularly important because a district court has ruled that the FTC staff cannot obtain information under the ECPA from ISPs during the discovery phase of a case, which limits the agency's ability to investigate spammers.[76]

2. Substantive Proposals. Substantive legislative changes also could aid in the FTC's law enforcement efforts against spam. Although Section 5 of the FTC Act provides a firm footing for spam prosecutions, additional law enforcement tools could make more explicit the boundaries of legal and illegal conduct, and they could enhance the sanctions that the agency can impose on violators. The Telemarketing and Consumer Fraud and Abuse Prevention Act ("TCFAPA"), 15 U.S.C. §§ 6101–6108, provides a model for addressing unsolicited commercial e-mail. Amendments to the TCFAPA would authorize the FTC to adopt rules addressing deceptive and abusive[77] practices with respect to the sending of unsolicited commercial e-mail. Approaching spam through this statutory model would provide the market with direction, but would do so within a framework that could change as the problems evolve. It also would provide several more specific, important benefits.

First, amendment of the statute would give the FTC general discretionary authority via rulemaking to address *deceptive* practices relating to spam. The rule would set out bright lines between acceptable and unacceptable practices for the business community. The list of deceptive practices could include: the use of false header or routing information; the use of false representations in the "subject" line; the use of false claims that an unsolicited commercial e-mail message was solicited; and the use of false representations that an opt-out request will be honored. As with telemarketing, a rule also could prohibit assisting and facilitating any of the above, *i.e.,* providing substantial assistance to another party engaged in any rule violation knowing or consciously avoiding knowing that such party is engaged in such violation.

Second, amendment of the statute would give discretionary authority via rulemaking to address *abusive* practices relating to spam. Specific abusive practices might include: sending any recipient an unsolicited commercial e-mail message after such recipient has requested not to receive such commercial e-mail messages; failing to provide a reasonable means to "opt out" of receiving future e-mail messages; and sending unsolicited commercial e-mail to an address obtained through harvesting or a dictionary attack.

Third, amendment of the TCFAPA would ensure that the Rule embodies the same standard of liability that is embodied in Section 5 of the FTC Act, without a general requirement to show intent or scienter. Imposition of intent or scienter requirements would unnecessarily complicate enforcement, and also would actually constrict the scope of the FTC's existing authority under Section 5 to attack spam.

Fourth, the amended statute would provide that the Rule would be enforceable, like all FTC Rules, through FTC actions in Federal district court, and it further would provide that violators would be subject to preliminary and permanent injunctions and could be ordered to pay redress to consumers. In addition, in an action brought by DOJ on behalf of the FTC, violators would be liable to pay civil penalties of up to $11,000 per violation (the amount of civil penalties is governed by statutory factors, such as ability to pay, previous history of such conduct, egregiousness of the conduct, etc.).

Like the existing statute, the amended TCFAPA would authorize states to enforce the FTC Rule in Federal court to obtain injunctions and redress for their citizens, but not civil penalties. The TCFAPA authorizes a private right of action for any person adversely affected by a violation of the FTC's Telemarketing Sales Rule if the amount in controversy exceeds $50,000 in actual damages for each person adversely affected by such action. The FTC, however, will need to assess whether the inclusion of an analogous provision in an amended TCFAPA that addresses spam would be appropriate, effective, and feasible.

Finally, the rulemaking authority granted through this amendment could be adapted to new changes in technology without hindering technological innovation.

An amended TCFAPA should seek to assure consistency between state and Federal laws. The scope of the Internet and of e-mail communication is global, tran-

---

[76] *See FTC* v. *Netscape Comm. Corp.,* 196 F.R.D. 559 (N.D. Cal. 2000).

[77] The FTC has determined, in the Statement of Basis and Purpose for the Amended TSR, that the undefined term "abusive" used in the legislation authorizing that Rule will be interpreted to encompass "unfairness." 68 Fed. Reg. 4580, 4614 (2003).

scending national boundaries. Congress should seek to minimize artificial barriers that would break up this market.

In addition to the TCFAPA amendments, the possible criminalization of false header and routing information should be explored. There is some debate over whether the wire fraud statute covers fraud in the sending of e-mail communications. The FTC staff is discussing this issue with criminal authorities to determine whether a specific statute that criminalized this conduct would clear up any statutory confusion or encourage spam prosecutions. At this time, the FTC has no recommendations on whether changes in the criminal code are necessary or appropriate.[78]

Admittedly, we recognize that these legal steps will not solve the growing spam problem. Nor is it clear what impact these steps will have on some of the other problems associated with spam (*e.g.,* volume and security). These issues may need to be addressed separately. Nevertheless, the FTC believes that the proposed legislation would provide more effective investigative and enforcement tools and would enhance the FTC's continuing law enforcement efforts.

D. Technical Changes

Finally, the FTC requests two new grants of authority: (1) the ability to accept reimbursement for expenses incurred by the FTC in assisting foreign or domestic law enforcement authorities, and (2) the ability to accept volunteer services, in-kind benefits, or other gifts or donations. Both new authorities would be useful as the FTC tries to stretch its resources to meet its statutory responsibilities.

The authority to accept reimbursement for expenses incurred would be especially useful in connection with the FTC's close coordination with domestic and foreign law enforcement authorities to address possible law violations. Partnering with these law enforcement authorities has resulted in enhanced law enforcement efforts and greater sharing of significant information. In some of these situations, the FTC's foreign or domestic partner is interested in reimbursing the FTC for the services it has provided or in sharing some of the costs of investigating or prosecuting the matter. Without specific statutory reimbursement authority, however, the FTC cannot accept and keep such reimbursements because of constraints under appropriations law.

In addition, the FTC requests authority to accept donations and gifts, such as volunteer services and in-kind benefits. Congress has conferred this authority by statute on various agencies, including the Office of Government Ethics, the FCC, and the Consumer Product Safety Commission. Without this authority, the FTC cannot accept services or keep items because of appropriations law constraints. This broad restriction on acceptance of gifts sometimes limits the FTC's ability to fulfill its mission in the most cost-effective manner. For example, the FTC cannot accept volunteer services from individuals wishing to provide such services to the agency. In addition, agency officials must sometimes refuse donated items that could otherwise be useful in carrying out the agency's mission, such as books and similar mission-related items.

V. Conclusion

Mr. Chairman, the FTC appreciates the strong support for its agenda demonstrated by you and the Subcommittee. I would be happy to answer any questions that you and other Senators may have about the FTC's reauthorization request.

Senator SMITH. Thank you very much.

Again, we apologize for the disjointed nature of this hearing, with all of the Senators having to come and go; but we appreciate your indulgence, because we have been able to continue on with your testimony.

If it is agreeable to my colleagues, we will do 5-minute rounds.

I am interested in pursuing further the whole issue of the common-carrier exemption. And, Mr. Muris, I believe it was in your testimony, where you stated that, quote, "The exemption has proven to be a barrier to effective consumer protection, both in common carriage and in other telecommunications businesses." You con-

[78] Any legislation that criminalizes certain types of spam activities should not negatively impact the FTC's existing Section 5 authority or change the present standards of proof, scienter, or evidence for cases of civil fraud, deception, or unfairness.

tinue by saying that, "The exemption has sometimes stymied FTC efforts to halt fraudulent or deceptive practices by telecommunications firms." Could you provide some specific examples of instances where the exemptions served as a barrier for an FTC action against a non-common carrier activity or telecom common carrier?

Mr. LEARY. Well, Senator, for reasons that should be obvious, we would prefer to provide the specific examples in a different setting than an open hearing like this, because I do not think it is fair to a potential company to identify the possibility that we might have brought an action against them, were it not for this exemption.

But we did have a situation that wound up in litigation in a case where both the FCC and the Federal Trade Commission agreed that we had jurisdiction. And yet the respondent disagreed, took the matter to court. We have, thus far, been successful in the preliminary—they made a motion to dismiss our complaint—we have been successful at that level, but that is still pending. And that is one reason why the mere fact that we can agree informally with the FCC on a particular matter is not conclusive, because some judge out there might read the statute differently. So that every time we have a situation where there is the possibility of that kind of an argument, that kind of a jurisdictional barrier, we have to confront it up front. It is an initial stumbling block for us. And I think we ought to be able to work out a solution to that problem.

Senator SMITH. Thank you. Will you explain what agencies, notwithstanding the FTC, are affected by your cross-border proposal, and describe their recent reactions to your proposal?

Mr. THOMPSON. Well, we have talked to some agencies. For example, we have worked together with the Department of Commerce, Department of State. We have also worked with the Department of Justice. We are talking to some of those agencies right now. We have some questions to answer, but we think that any questions that we have, we will be able to work through.

I think that there is a general understanding of the importance of the need to streamline and update our ability to share information so that we can prosecute cross-border fraud cases, because it has grown of greater importance to our consumers to be able to provide them with remedies for transactions that they engage in that involve parties outside of our country.

Senator SMITH. And I am wondering, as we contemplate your proposal, as it relates to cross-border fraud, you have requested exemption from FOIA, the Freedom of Information Act, that it is somehow necessary to be exempted from that. Can you speak to that further?

Mr. THOMPSON. I can, briefly. You know that, for law enforcement, that there is a general exemption that we have for FOIA for investigations that we conduct, but it is not entirely clear that if it is information that we get pursuant to our relationship with another country, that they share with us their law enforcers, that that would be worthy of a similar protection. This clarifies that, so that—what we are concerned about right now is information—for example, from a foreign law enforcer—that really deals with our citizens or activity that takes place here, we cannot get that information at all. And unless we have some way to protect the integ-

rity of the investigation—that includes witness statements, expert testimony—then we need that information so that we actually know what is going on and that we can protect our citizens.

Senator SMITH. Thank you.

Mr. Muris, your Commission has a range of consumer-protection oversight, obviously, and one of the things that any parent is concerned about is these peer-to-peer file-shared Websites, like Kazaa, Morpheus, Grokster, which lure unsuspecting minors to look at free access to their supposed copyrighted material under words like "Harry Potter" or "Britney Spears," and what they find is not kid-friendly at all; it is grossly pornographic. And I am wondering, is this deceptive trade practice—it seems to be under the FTC's jurisdiction, under Section 5, which prohibits or prevents unfair or deceptive trade practices—have you looked into this growing problem? And do you have a solution that can help us, as we go into the future, to protect our young people from what is clearly deception when it comes under the heading of "Harry Potter" and is just pornography?

Mr. MURIS. Well, we have found, quite frankly, some very disturbing things in this area, and we have just begun to look at it. We will be addressing—we are doing a follow up report, at congressional request, on the marketing of violent entertainment media, and we are looking—in that report, we will be looking at the extent to which this new channel for distribution of these products is used.

We are looking, specifically, at the question that you mentioned. We find, in some of these areas, unfortunately, they are quite explicit about what they are leading you to, and, in that sense, not deceptive.

On the other hand, we have found—and this fits in with a lot of what we are talking with spam, deception, with what we do—we have had some startling examples of deception leading to pornography. For example, we found a spam that said, "Win a free Sony Playstation." And in five clicks of your mouse, you were on a pornographic Website, where your phone bill was being billed to a 900 number, and all that was happening in a deceptive fashion, and we shut them down. So we are still in the midst of looking at this area. But unfortunately, you know, what we are finding is not very promising, from the perspective of parents.

Senator SMITH. I am going to turn this over to my colleague, Senator Wyden, but I—along this line of questioning, I am also concerned that consumers who use these software devices—in tapping into these things they also expose their own private materials—health information and other things—to the general public domain. And I think somehow there has got to be a way to find some protection against that.

Mr. MURIS. Well, yes, Senator. And you are absolutely right, there are very serious, more general privacy concerns beside the concerns that we were discussing, in terms of children.

Senator SMITH. Thank you.

Senator Wyden?

Senator WYDEN. Thank you, Mr. Chairman.

Mr. Chairman, first, on the spam-enforcement issue, I do think that Congress is going to pass an anti-spam bill with criminal and

civil penalties into it. And the question then becomes enforcement. And I am of the view that bringing several high-visibility, major enforcement actions against these significant spammers would send a very significant message of deterrence and that things would be different. I would like to know if you agree and if you will commit to the Committee today that if the Congress passes legislation, with real penalties that are civil and criminal, that you will make it a high priority to go out and bring several significant enforcement actions, so as to actually get a message out there that there is going to be some deterrence.

Mr. MURIS. Well, first of all, Senator, I think I want to compliment you for being a prophet ahead of your time. You have been pushing this issue legislatively for years. We have made attacking deceptive spam—and, unfortunately, the overwhelming majority of it is deceptive and fraudulent—a priority. Certainly, if legislation is passed—particularly, we hope, legislation would give us some new procedural authority making it easier for us to investigate—that would be helpful. Commissioner Swindle may want to comment on this, as well.

I am agnostic, at best, about the impact that we would have with cases. We are bringing cases. We are actually working with U.S. attorneys to bring—they would bring criminal cases. We just do not know if there are thousands of spammers or if it is concentrated in a relatively small area. We do know they cannot be traced through the Internet. They have to be traced by following the money trail. So we are committed now to increasing our efforts to go after them. I think new legislation would be helpful. But I just cannot answer the question whether—you know, of what the impact would be, given our ignorance about what is going on in the spam world.

Commissioner Swindle, did you want to——

Senator WYDEN. Well, and maybe Mr. Swindle wants to get into this.

I mean, it seems to me, right now—we heard this from the spammer—it is pretty much the cost of doing business. I mean, it is not considered any big deal. And what I want to do is send a message that the world is different, that this will be treated as something that faces serious sanction.

One of the things I am proudest of—with Senator Specter, I wrote the Armed Career Criminal Bill. It was discretionary. But when prosecutors brought a relatively small number of cases, and career criminals saw that the world was different, it actually began to make a difference on the ground.

And what I want to see is a Commission that is going to say, "If Congress passes a law, we are going to go gangbusters," in terms of trying to send an enforcement message that there is some teeth out there. Because nobody thinks there is any teeth right now.

Commissioner Swindle, did you want to add to that?

Mr. SWINDLE. Senator Wyden, first I would like to assure you that we are incredibly serious and professional in implementing our law enforcement role and enforcing the laws that the Congress passes. Please do not question that—I want to assure you that we are—I mean, I have been associated with the agency for 5 years. I have never met a more professional group of people in my life

than those who work at the Federal Trade Commission. I mean, they are earnest, they burn the midnight oil. We expend enormous resources, and people literally work over there overtime without the pay. I mean, this is a professional outfit, and we are very earnest about this, and we do pursue them aggressively.

History teaches us, at the Federal Trade Commission, that there must be at least 100 scams in the world. At least 100. I am being a little facetious, because there is probably millions of scams. We have had a number of recently—a number of relatively good hangings, with regard to law enforcement. And it does have a deterrent effect. But the scams keep going on. We are seeing scams that have been around, certainly since my childhood. They have just taken a new form.

So I think narrowly defined new legislation that more accurately defines the problem, what is right and what is wrong, I think those kind of things can help. And, as I said, many of the suggestions that we make in our formal testimony, written testimony, are incorporated in Burns-Wyden, and we want to see less ambiguity about what is right and what is wrong in this business.

Unfortunately, it is not as simple as some of the other scams that we have seen, where there are, sort of, finite constraints. There is a boundary. There are a limited number. Here, we have a phenomenon, a means of scamming people that is boundless, it is open. The technology is literally open, and that may be one of the problems.

The point is, we have got to have strong law enforcement; solid, narrowly defined laws that do not do more damage than they do good. And we have to have technology improvements. And we have to have aggressive people pursuing it, and industry leading the way to find some solutions, also. I can assure you, from the FTC's standpoint, we will be pursuing things aggressively. And if new laws are passed, we will——

Senator WYDEN. Let me just see if I can——

Mr. SWINDLE.—be pursing those aggressively, also.

Senator WYDEN.—I can get into one other area before the light goes off.

Nobody is doubting the intentions and the professionalism of the FTC, Commissioner. The problem is, a spammer sat right where Mr. Leary is, just a couple of weeks ago, and he said, "There are essentially no restraints on us today, and there are not any hangings going on." That is what the fellow said, sitting next to him. That is what I would like to try to change. We are going to see if we can get you the tools. I want a commitment for enforcement.

If I could, Mr. Chairman, just one question on the gasoline-prices issue.

Chairman Muris, you all have been monitoring gasoline prices for a year now. But as far as I can tell, there has not been an action to protect the consumer. And in fact, the Federal Trade Commission's action against Unocal was for misrepresenting to the oil industry about its research. And I was struck, even in your testimony, you talk about how you are helping industry participants. Your concern there was industry, rather than the consumers that Senator Smith and I know are getting shellacked all up and down the West Coast.

So my question is, What is it going to take to get the Commission to do something to help the consumer, the people on the West Coast of the United States, who are consistently getting the highest gasoline prices? You all found that there were anti-competitive practices in the West Coast market. That was a finding in your West Coast study. And you have done something that is of value to industry. And I am certainly in favor of stopping misrepresentation. But I would like to know what you are going to do to help the consumer.

Mr. MURIS. Well, Senator, this is the third year in a row in which there has been a hearing. And I know you sent us a letter, that we received yesterday, where you have been largely critical of the Commission's practices. Most of what you have been critical of, I had not been a part of. So after last year's hearing, I committed to personally spend many hours on this issue with de-novo review, if you will.

First, it is simply not true that we have not done anything. The Commission, for example, since 1997, has acted in over 150 energy-industry markets requiring divestitures in merger cases. No other industry is the Commission—these are the largest and most extensive divestitures.

Second, the Unocal case—let me talk about the complaint; the case is in litigation, so let me just stick to the complaint—it is about protecting consumers. Everything we do is about protecting consumers.

Senator WYDEN. At page 31——

Mr. MURIS. The alleged——

Senator WYDEN.—of your testimony——

Mr. MURIS.—the alleged misrepresentations were to the California regulatory authorities that harmed consumers. And the way they harmed consumers—again, according to the complaint—was that Unocal offered to give this technology without charging for its intellectual property. The industry did rely on that. They invested. And then Unocal said, "We want royalties." Well, that harmed the companies, but that harmed the consumers, because the—and that is what we care about. The allegation is, the consumers were harmed because the royalties get passed through to the consumers.

Senator WYDEN. Well, again, I would just refer to page 31 of the testimony. Your concern there was, there was a misrepresentation to industry participants. I still cannot find anything that is going to be of any value to West Coast consumers. My door remains open to you to have an opportunity to work with you. As you know, I presented a proposal to you, and I thought we were ready to go forward on a bipartisan basis, and I would still like to do that.

Mr. MURIS. Well, if I——

Senator WYDEN. Thank you, Mr. Chairman.

Mr. MURIS. Could I respond, Mr. Chairman?

Senator SMITH. Yes.

Mr. MURIS. In fact, one of the things we did—I know you are concerned about zone pricing—we asked the Interdisciplinary Center for Experimental Economics at George Mason University to look at this issue. It is headed by Dr. Vernon Smith, who is last year's Nobel Laureate in Economics. To date—and they are not quite fin-

ished—but what their work has shown is that zone pricing lowers prices; it does not raise prices.

Zone pricing provides—I said I would to a de novo review, and that is—and I am telling you where the evidence has led us—zone pricing provides suppliers with a way of preventing dealers who have location-specific advantage—and that happens all the time; you will have a dealer, because of zoning or some advantage, can charge higher prices—it prevents the dealers with a way limiting the dealers from reaping the benefits of those advantages.

The focus on zone pricing and the proposals that you have made, I think, would actually lead to higher prices, not lower prices.

Senator WYDEN. Mr. Chairman, my time is up. I would like to make part of the record the study that Mr. Muris is talking about.

[The information referred to follows:]

The final version of FTC Working Paper 263, Experimental Gasoline Markets (February 2006), by Bart Wilson and Carey Deck, can be found at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=445721&download=yes*

Senator WYDEN. The proposition that zone pricing is good for the consumer is one of the most farfetched ideas I have heard in my time in the U.S. Congress. I look forward to——

Mr. MURIS. Well, can I respond again, Mr. Chairman?

Your premise is a premise that had a lot of support in the antitrust laws 35 or 40 years ago. And the premise was that intrabrand competition—that is, competition between dealers—is what the focus of the antitrust law should be.

Since then, we now focus on inter-brand competition. In other words, instead of focusing on competition between McDonald's franchisees, we focus on competition between McDonald's and Burger King and the others.

And in fact, by focusing on that inter-brand competition, I think we provide more benefits to consumers. And the position that I think, after your letter, I now understand you to be espousing, is a position that has been repudiated in the antitrust laws, beginning with a Supreme Court decision, in 1977, which reversed a 1967 Supreme Court decision, and it is now widely recognized that the focus needs to be not on McDonald's effort to tell its—to restrict competition between McDonald's franchisees, but on competition between the inter-brand firms, between the gasoline refiners, between McDonald's, Burger King, et cetera.

Senator WYDEN. Mr. Chairman, my colleagues are anxious to ask their questions.

The current law, so that we are aware of it, is that people similarly situated have to be treated in a similar way by a company. That is the current Supreme Court decision. That is why zone pricing has been so pernicious.

And I want to let my colleagues ask their questions. And I am certainly interested in hearing how, somehow, something that has resulted in huge damage awards in our State essentially as an anti-competitive thing, is judged by Chairman Muris as somehow good for the consumer.

And I thank my colleagues.

Senator SMITH. Senator Dorgan?

Senator DORGAN. Mr. Chairman, let me ask members of the Commission whether you think we are losing the battle on spam. I ask that because, as a parent struggling through parental controls on ISPs, with two teenage children, my observation is that even as we talk about this battle to deal with spam, we are losing, in a very big way, and losing very rapidly. Would you all agree that we are, at this point, losing the battle in a significant way?

Senator, I certainly would comment on that, and I made reference in my opening remarks—I am not sure the Senator was here—but I said we may be seeing the killing of a killer application for the Internet, Web-based services, right now, because as much as we have been looking for that one thing that is really going to make broadband take off, we still have not found it. But the thing that is popular is E-mail and E-commerce. People—we all shop on the Internet, and this nature—and people are getting fed up with even doing that, because there is so much spam.

We are not going to lose this battle, but we may lose untold opportunities from people turning away at this point in time and us not capitalizing, in an economic sense, on the benefits of this technology because they have gotten fed up with it.

So I think we have got to just redouble our efforts. It is going to take a combination of a lot of things. I have been a great supporter of industry, in the information-technology industry, certainly, trying to avoid onerous laws for privacy and these things. While I think they are very important, we have to be careful how we do it, because the industry changed so quickly that laws passed to day may very likely have more adverse effect tomorrow than they will do good.

But at this point in time, I think there are things that industry can do—and I have so much as said it, I think, in this testimony—that they can provide to consumers and end-users an ability to be in control—that end-user be in control—of what comes into their computer, in the form of E-mail and——

Senator DORGAN. Well, let's hope that is the case, but that has not been the case so far.

Mr. SWINDLE. That's right.

Senator DORGAN. The fact is, this problem is growing exponentially worse, not better.

Mr. SWINDLE. Yes, sir.

Senator DORGAN. We are not even holding our own. It is getting much, much worse. It is disgusting, it is intrusive; and the fact is, we are losing the battle.

Mr. SWINDLE. Yes.

Senator DORGAN. And I do not at all question the interest of the Federal Trade Commission in dealing with this. I think you want to deal with it. We want to deal it.

Commissioner Muris, you indicated that we are not able to find the location of the sender, except by tracking the money. Can you give me some indication of what kind of investigative effort is underway at the FTC? What kind of resources, what kind of money? Is this——

Mr. MURIS. Sure. I——

Senator DORGAN. Is this a big-time investigation going on? And if so, what is the result of it?

Mr. MURIS. We have, as part of—since I have become Chairman, we have now easily doubled our resources in privacy in general, and spam has been a part of that. Obviously, we do not——

Senator DORGAN. What does that mean, double your resources?

Mr. MURIS. You mean how many people?

Senator DORGAN. From one to two? Or——

Mr. MURIS. No, no, no. We are——

Senator DORGAN.—from 100 to 200?

Mr. MURIS.—talking where we were spending 30 to 40 FTE and several hundred thousand dollars in support to—close to or not more than doubling the FTE, and the support has probably gone up, you know, by an order of ten times. This is on privacy, in general.

Now, on spam, we have—and we are trying to do what Senator Wyden asked, in terms of—in Commissioner Swindle's eloquent phrase, "public hangings"—because I agree, that is what needs to happen here. We are working with some U.S. attorneys, because obviously the criminal sanctions are tougher than sanctions that we can apply. Just to find someone, because you cannot track them through the Internet, takes multiple CIDs. And one of the frustrations of this—that is our term for a subpoena—one of the frustrations of this is, you do not know—in many law enforcement investigations, when you start, you have some idea of what you are going to find. Here, you do not know whether you are going to find, you know, a couple of hundred guys out there, a couple of big guys. You do not know until you start. And that is frustrating.

The economics of spam—you are absolutely right, we are losing the battle, which is why it is going to take a multifaceted approach. I absolutely agree——

Senator DORGAN. But my question, Mr. Commissioner is—the resources that you are devoting to these investigations—I am wondering—I think Senator Wyden was asking what additional authority you need.

Mr. MURIS. Uh-huh.

Senator DORGAN. And I am asking what additional authority do you need, and what additional resources do you need? Because you cannot wage this war against spam—and, believe me, it is a war we are losing at this point—if you have got 15 or 20 or 25 people against billions of E-mails spammed every single day. I mean, so the question is, What kind of resources are you committing, and what do you need?

Mr. MURIS. We cannot solve the problem by ourselves, no matter how many resources that you give to us. We are spending numerous FTE and much support money on this. We are working with our partners in the States. We are working with two U.S. attorneys on spam-specific criminal investigations.

This is going to take an approach of technology, of consumer education. It may even take some basic changes—I hope not, because they are complicated to do—some basic changes in the way the Internet works.

I think we are on the same page here completely. I have never seen a consumer-protection problem this difficult.

Senator DORGAN. All right. Two other quick items, and my time is about up. One, with regard to the common-carrier issue. I as-

sume you are still in discussions with the FCC about an MOU on that. That is, I think, a very important issue. And I wanted to just mention one thing, and you can respond to that.

I noticed, the other day, with great fanfare, the indictment of Martha Stewart. And that, of course, was—in the 24-hour, 7-day-a-week news cycle, was big news. I met with you, Mr. Muris, and a couple of other Commissioners, at the time that I was chairing hearings dealing with Enron. And I find it fascinating and somewhat—more than somewhat—I find it really disappointing that Mr. Kenneth Lay and Mr. Skilling, who sat at the table you sat at, are still sitting behind their gated communities. They ran a corporation that, in my judgment, bilked the stockholders and employees out of a substantial amount of money. I see no legal action with respect to some of the biggest targets, with respect to the Enron Corporation, and yet prosecutors move with Martha Stewart, in a very high-profile situation. I do not know Martha Stewart. I mean, I do not watch her programs and do not know much about her.

But I met with you, because I was curious why the FTC did not have a piece of the action with respect to investigating a company whose executives were telling both the employees and the public, "Buy this stock, because it is going to go up. Buy this stock. It is a good value," at the same time they were selling their stock, and at the same time they were running that company into the ground and were creating a hollow shell and, you know, a financial picture that was, in my judgment, criminal.

And I only say this to you in the hope that we can still find a way for the FTC to be relevant on these issues. You told me why there has been this understanding, over decades, with another Federal agency, but the——

Mr. MURIS. Well, sure. In fact, the SEC literally, literally, came out of the FTC. Two commissioners and a couple of hundred employees went over and started the place. So——

Senator DORGAN. I understand that. My interest is in seeing that you, at some point, can claim a part of the responsibility to be involved in this, because, you know, I am not really happy seeing the lack of results in this with the SEC.

And so, having said all that, I just wanted to put on the record—we had a long discussion about this on, I think, two occasions. And I think it is right in the center of the bull's- eye, what the FTC ought to be concerned about, as well. And I know that you—at this point, and for customary reasons, you have deferred to the SEC, and you point to the law and some other things that suggest that you cannot be involved.

But having said all that, would you just tell me that you are involved with the FCC on the common-carrier issue, still involved in discussions with an MOU on them?

Mr. MURIS. Yes, Senator, we are. You have been a very good friend of us, and you were in your chairmanship, and you continue to be. I understand your point. It is, I think, for the reasons that we discussed, an area on which I thought deference was appropriate by us. I think we have been very aggressive in the areas that we have within our call. I do think, as Commissioner Leary was discussing, because of our expertise dealing with advertising,

we would be a natural in the common-carrier area to deal with those issues, as well. And that is why we are asking for your help.

Senator DORGAN. Yes, well, just one final point. On both spam and on the issue of corporate malfeasance and so on, I think, to the extent you can, you should walk loudly and carry a big stick. And my colleague talked about public hangings. He meant that in, I think——

Mr. MURIS. That was Commissioner Swindle.

Senator DORGAN. Yes, we will pass it off——

Mr. SWINDLE. It is an old Marine Corps term.

[Laughter.]

Senator DORGAN. We all know what you meant by that. But walking loudly and carrying a big stick is very important in battling these kinds of actions, and I hope you will do that.

Senator SMITH. I think Senator Dorgan wants you to find a Martha Stewart of spam.

Senator DORGAN. Or an Enron executive of spam.

[Laughter.]

Senator SMITH. All right, thank you.

Mr. MURIS. We will look. It would not surprise me.

Senator SMITH. Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. I commend Commissioner Muris and his colleagues for having made this agency truly a law enforcement agency, doing a good job. And this is kind of a first touch with me in my second round in the U.S. Senate, so I am happy to see you again.

And just a couple of questions. I noticed that, in the statement that was offered here by you, that you referred to protections for children, Spanish-speaking, consumers, the military, and so forth. The elderly are a particularly susceptible group. Do we have specific programs to protect the elderly from deceptive practices, fraud, et cetera?

Mr. MURIS. Absolutely, Senator. We work very closely, for example, with the AARP. They have been very supportive of us. They were extraordinarily supportive on the Do Not Call list, for example. We have worked closely with them in trying to work with that particular population. As you know, it is a fairly diverse population, actually, in terms of their susceptibility to some of the problems. But there are scams that are aimed especially at them, and we pay special attention to that.

Senator LAUTENBERG. I hope so. And it is not because I am part of that group. I take care of myself. But there are other——

[Laughter.]

Senator LAUTENBERG.—they may need some help.

I want to ask you, is telemarketing a legitimate business?

Mr. MURIS. If you look at the size of the telemarketing, and contrast it with the spam business, the size of the telemarketing business is a very legitimate business. B-to-B, for example, business-to-business, is bigger than business-to-consumer. The part of telemarketing where—you know, I recently saw—I grew up in California in the 1960s; I think Senator Wyden did, as well—I recently

saw a Beach Boys tape. You know, it said, “Call a 1–800 number.” I called it and ordered the tape. That is a bigger part of telemarketing than when they call you—you know, the kind of calls we are restricting on Do Not Call.

Charitable fundraising is obviously a very big part of telemarketing. Political fundraising is a big part of telemarketing. Surveys are a big part of telemarketing. All this, I think, is in pretty stark contrast to what we are finding in spam, where we have got a world of fraud and deception.

Senator LAUTENBERG. Yes. No, I had enough spam when I was in the Army, and I am not looking for more.

[Laughter.]

Senator LAUTENBERG. I can tell you that, in the process—and I feel as strongly as do my colleagues about eliminating spam as much as we possibly can. But the fact is that if it is a legitimate industry, are we doing anything that protects the legitimate purveyors, or at least lets them operate without being harassed by the FTC?

Mr. MURIS. Well, one of the things that has happened is—unlike telemarketing, again, we could do a Do Not Call list in telemarketing, because we are dealing, overwhelmingly, with legitimate businesses.

In spam, we did a—one of the things I had our staff do—we collect spam. We are the only people in the world that like to get spam. We get over 120,000 a day now. And we look through a random sample of spam. And we have found, without looking hard, two thirds of them were deceptive; and, certainly, a bigger percentage of the others were. Most States, or a lot of States, including California, a very big State, already requires spam to be labeled ADV or some variation of that. Only 2 percent of the spam follow that, and you know everybody sending spam has to be sending it with—you know, some of it is going, at least, to California.

We are dealing with—it is quite possible that if we somehow cleaned this up, maybe we would have a situation where we had a lot of legitimate businesses, and we could do some of the regulation that we have done in telemarketing, but that is not the situation we face now.

Senator LAUTENBERG. I am curious about tobacco. And are you reviewing the claims made by tobacco companies about low-tar cigarettes? And what are you finding, if you have been?

Mr. MURIS. Well, the Commission—this is an issue—I was involved with it at the Commission when I was head of the Bureau of Consumer Protection in the early 1980s. This is an area—the Commission started, with Congress’ ultimate blessing and through various lawsuits, the tar-rating system. And it is broken.

And what the Commission, under the previous chairman, Bob Pitofsky, asked, was to get the scientific agency—sent a letter over to HHS to get the scientific agencies to fix it. In fact, we think it ought to be run—or that the Commission, in that letter—and I have endorsed this—think it ought to be run, the tar-rating system, by those agencies. NCI issued a report in 2001, which just affirmed what we knew, that the system is broken, and we now hope that they will work with us and the more science-based agencies to try to fix it. Because there is no doubt that because of what is called

"compensation," consumers smoke lower-tar cigarettes harder than they smoke higher-tar cigarettes——

Senator LAUTENBERG. Right.

Mr. MURIS.—so that the proportional—you know, they do not get what you might think, in terms of proportional delivery—that there are serious problems with the system.

Senator LAUTENBERG. What do you think can be done to expose the problem more obviously? Right now, there is a seduction process to get people to the low tars. And again, it really is not a safer product for one's health. But the advertising goes on, and it attracts a lot of new smokers.

You know, I was very active in anti-tobacco use in my previous term. And when we started with the ban on smoking in airplanes, it kind of revolutionized the approach of the whole industry and the view of tobacco, and I think it has been very helpful.

I want to ask you this. Given the fact that the industry continued to advertise the Joe Camel image, despite the FTC's effort in the 1980s to stop the campaign, do you now think that you have the kind of authority, the regulatory authority, that is necessary to stop the current or future harmful targeted tobacco advertising, such as Joe Camel?

Mr. MURIS. Well, the Commission has authority. The Commission actually brought a complaint against the Joe Camel advertising. Many of those issues are now covered by the agreement between the tobacco companies and the States, and where the tobacco companies have agreed to do less of some of the kind of advertising that they did before.

We certainly have the substantial ability to deal with deceptive advertising, and we will continue to do that. There are obviously many issues involved of a scientific nature, such as the tar system I was just talking about, about which I think the scientific agencies are better able to deal with than we are.

Senator LAUTENBERG. Thanks, Mr. Chairman. Thank you very much for your——

Senator SMITH. Thank you, Senator Lautenberg.

I know we have a second panel. I have one brief question. My colleagues may have additional questions, as well.

You have mentioned the Do Not Call list. I am wondering if there is a Do Not Spam list and whether that would be effective?

Mr. MURIS. Well, for a couple of reasons, at the moment—for at least three reasons—we have a lot of skepticism about a Do Not Spam list. One is—that I was just talking about a minute ago—there is so much of this that, unlike telemarketing, we are dealing with people who are already breaking the law. I would, personally, at the moment, be very reluctant to have my name on it, to have my E-mail on a Do Not Spam list, because I would be very afraid the spammers would get it. And third, there is a finite number—there is some technological problems we would need to explore. We do not have a definitive view on this. But there is a finite number of telephone numbers, relative to the combinations and permutations you can do with E-mail addresses, and it may be that the number would be so large it would become unmanageable. I am not say we know that for sure, but that is a significant difference be-

tween—those, combined, are significant differences between Do Not Call and Do Not Spam.

Senator SMITH. Commissioner Swindle, do you share that view?

Mr. SWINDLE. I would go so far as to say I do not think there is any practical way to even consider that. With all the things that we can do——

Senator SMITH. Might there be a technological invention coming along that would make that——

Mr. SWINDLE. I do not hear it from people in the industry that I talk to, and I am constantly challenging them to solve these problems, to empower consumers. And nobody drifts over to that approach——

Senator SMITH. You have heard nothing from the high-tech industry, in terms of a technological fix to Do Not Spam?

Mr. SWINDLE. I have not heard anything, and I am highly skeptical if it could be arranged.

Senator SMITH. Thank you very much.

Senator Wyden?

Senator WYDEN. Thank you, Mr. Chairman. Just a couple of other online questions.

The Commission talks, in its testimony on spam, that they seek support for the development and deployment of technological tools to fight spam. I assume you all are not talking about subsidies from, you know, the Congress to fight spam. But I am curious what kind of support you want the Congress to provide.

Mr. SWINDLE. In the battle against spam?

Senator WYDEN. I am quoting from your testimony, Commissioner. You are saying a spam solution should include, and I quote, "support for the development and deployment of technological tools to fight spam." My question is, What kind of support do you want Congress to provide?

Mr. SWINDLE. Well, one of the things I, personally, think that Congress could provide is—you have many dealings with industry. I think we need to elevate this issue, through—what is the proper word here?—"jawboning," that might be an appropriate word. I think everybody is in this together, and we have to solve this problem for our collective good. We need to get the best possible solution. Legislation alone is not going to do it. Technology alone is not going to do it. We have an enormous awareness challenge here of educating consumers and small businesses and large businesses and everybody involved with it, that there are just certain things we have to do.

And this goes further than just spam, Senator, as you well know. So much—in fact, I think a large proportion, if not the vast majority of, the viruses and Trojan horses and malicious code that are spread, are spread through spam, and this gets beyond just the nuisance that you and I experience, and Senator Dorgan is terrified of because of his children. It goes into the capacity to literally shut down our critical infrastructure, which really gets into big bucks.

And we are talking—I heard someone quote a figure the other day, I think, in our Spam Forum, that spam, in this country this past year, would cost something up to the tune of $10 billion. That is high crime, as far as I am concerned.

Senator WYDEN. I just wanted to make sure that when you were talking about congressional support, you were talking about something along the lines that you have mentioned and not something where somehow we were supposed to be spending money.

The only other question deals with an Internet privacy issue. Obviously, a lot of companies have privacy policies that are online, and a lot of the stuff is just incomprehensible. I mean, it just goes on and on and on in legalese and gobbledygook. You all have been concerned about it in the past. We are concerned about self-regulation.

My question to you—maybe the Chairman wants to get in this, as well—how do you all find out if a company is violating its posted privacy policy? In other words, they have got something online, and it goes on for pages and pages, so it does not help consumers that way. And then I am curious what you do to find out if they are even complying with what they said they would do.

Mr. SWINDLE. Well, obviously, consumer complaints——

Senator WYDEN. Right.

Mr. SWINDLE. Eli Lilly is a good example of where a privacy policy was, I think—as it turned out, through their own carelessness—was violated, and some very personal information was revealed through lousy internal controls. But I think we get most of it probably from consumer complaints. It would be impossible for us to monitor all companies. In fact, I think that would cause a lot of alarms to go off.

But I think, in all honesty, we have been talking privacy, as the Senator certainly well knows, for five or 6 years now, and the chatter, the constant debate, the constant disagreements and eventual agreements on different things, has made the general public aware. The general public now is saying to firms, "If I am going to do business with you, especially in the online world"—and this obviously has an application to the offline—"you had better respect my privacy and how you deal with the information I give you." Once consumers start demanding that, business will react.

And business has reacted. You know, we have less privacy laws here than they do in Europe, and I have seen at least one survey, and I think I saw it repeated a second time, saying that we do a better job here, about protecting people's privacy and posting good privacy practices, than they do in Europe.

One, I think, heartening note is, there is a group of people in the industry right now looking at ways to make simplified privacy notices, that I think has a lot of promise. And it is being bandied around now. I know it is going to be a topic of discussion down in Australia in September, when I am down there with Privacy Commissioners, by those who are working on it.

So I think we are making progress. I agree with you, some of these privacy notices are absolutely insane. Some of the ones we get in paper from our credit-card companies are even more insane than the ones online. We have got a long way to go, but I do not know that we get there by snapping our fingers. I think it is going to be an evolutionary process, and back again to that support that leaders like you can give us by saying, "Get this done."

Mr. MURIS. Senator, if I could just add one—I agree with what Commissioner Swindle is saying, but one point—and for this, is

something I am very grateful for you—our mutual friends in the privacy groups, many of whom are here today. I know you introduced me to many of them early on in my chairmanship, and they have been very helpful in this area in bringing these problems to us. And we have, on occasion, done some looking on our own. And as you know, we have started, under my chairmanship, doing something that has not been done before, which is going after these security problems. We have brought three cases. And I will not use Commissioner Swindle's eloquent phrase, but those clearly have gotten the attention of everyone in the same way that you want to get the attention of the spammers.

Senator WYDEN. The Chairman has got a long afternoon ahead of him, so I am not going to go into this any further. I think what concerns me, because I do very much support the self-regulatory efforts that Commissioner Swindle is talking about. I think we saw that, in 2000, the Commission said that we really needed some kind of baseline with respect to online privacy, and I would hope that the Commission would continue to look at trying to figure out a way to do that so as to not burden the many responsible companies that are out there, but also to deal with the scofflaws. Because the problem is that you can have 90 percent of the people, plus, playing by the rules and being straight with the consumer, and the 10 percent can inflict a tremendous amount of damage.

And the only exception I would make to what both of you have said in this area is, we should not have to wait until you have an Eli Lilly disaster before a consumer-protection effort kicks in. You want to do something before you have that. And I think you know that, and I do not think you intended it to come out that way, Commissioner. And——

Mr. SWINDLE. But Senator, I can assure you we are not waiting on another Eli Lilly. We are busy at work——

Senator WYDEN. No, no.

Mr. SWINDLE.—day in and day out, and we will be. And thank you for your support.

Senator SMITH. Thank you, Senator Wyden.

And to our distinguished panel of Commissioners, we thank you for your participation today, and we will dismiss you, with our appreciation, and call up our second panel.

It consists of Mr. Mark Rotenberg, Executive Director, Electronic Privacy Information Center; Ms. Susan Grant, Director, National Fraud Information/Internet Fraud Watch; Ms. Sarah Deutsch, Vice President and Associate General Counsel, Verizon Communications; Mr. Larry Sarjeant, Vice President and General Counsel of the U.S. Telecom Association; Mr. Scott Cooper, Manager of Technology Policy at Hewlett Packard, and Mr. Ari Schwartz, Associate Director, Center for Democracy and Technology. Welcome you all.

Why don't we start at Mr. Rotenberg's side of the table, and we will just go across, and thank you all for your patience today as we had this important hearing and dealt with a lot of other Senate business simultaneously.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC); ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman.

My name is Marc Rotenberg, and I am Executive Director of the Electronic Privacy Information Center. We are a public-interest research organization here in Washington. We work in close association with consumer and civil-liberties organizations, both in the United States and around the world, on emerging policy issues.

And I would like to thank the Committee for drawing attention to the problem of cross-border fraud. This has clearly become an important issue. As the use of the Internet has increased, commercial opportunity has increased; but so, too, has the opportunity for consumer fraud.

And I also wanted to recognize the work of the Federal Trade Commission, the chairman and the other members, for their efforts over the last several years to focus public attention on this issue, to work with consumer organizations, and also to work in association with the Organization for Economic Cooperation and Development, which we think is a very important policymaking forum, particularly as these new issues arise.

I am going to focus my comments today on a draft legislation, the so-called Internet Consumer Protection Enforcement Act, which I believe is being considered as Title III of the FTC reauthorization. This draft bill, which has been put forward by the FTC, would facilitate an important effort to enable cooperation among consumer-protection agencies around the world. And we certainly support that, and I want to make clear our support for this effort. At the same time, I would like to draw your attention to a few concerns we do have about the draft bill, particularly the impact that it might have on privacy protection and open Government as the U.S. works in cooperation with foreign law enforcement agencies. And I would also like to make a few general comments about privacy protection, going forward, at the FTC in the context of the reauthorization.

But I am going to focus, really, on three critical issues related to this draft legislation and urge you and the other Members of the Committee to consider making some changes. As I said, we think this is an important effort that should go forward, but some changes, we believe, will be appropriate.

Now, what this legislation attempts to do is to enable data sharing, investigative files and information between the FTC and sister agencies in other countries, so as to go after people who are taking advantage of the Internet to commit fraud and to basically hide behind other jurisdictions to make it more difficult to locate them. So to solve this problem, you clearly need to have some cooperative relations and some agreements about this sharing of the investigative information. But it is important, in doing that, that we do not sacrifice some of the privacy safeguards and procedural rights that exist in the United States.

For example, as a general matter, we would provide a notice to the target of a subpoena, so that the person who is going to effectively become the subject of the criminal investigation might be

given the opportunity to oppose, if this was appropriate and necessary.

There are provisions in the draft bill that essentially remove those notification requirements, and the argument is made that this is necessary so as not to tip off the target. But you see, that argument could be applied just as easily within the United States, and we do not think this is a good precedent. We think it will also send a bad message to law enforcement agencies in other countries about how the United States pursues criminal investigations.

I wanted to draw your attention also to some proposed changes in the Freedom of Information Act, which, for us, is a very important law. It enables public oversight of the activities of Government, allows us to assess how well Government agencies are doing their job. The FTC is proposing, in this draft bill, to create new exemptions that would allow them to withhold information that would otherwise, because it is public-record information, be available to the public if they choose to go after it.

Our view is that these exemptions are not necessary, because the FTC currently has authorities, under the current exemptions, to withhold information that might be, for example, used in a current ongoing investigation—that is the (7)(a) exemption—or that might be obtained under a confidential agreement from a foreign law enforcement agency. That is the (7)(d) exemption.

And I should mention that my group, EPIC, has particular experience with how the FTC uses these exemptions under the Freedom of Information Act, because we have requested information from the agency in our own efforts to assess how well they were doing their job. And they withheld some of the documents that we sought, citing just these same exemptions, or at least citing the (7)(a) exemption.

So our view is that they know they have these exemptions. They know how to use these exemptions. We may disagree about whether or not they are properly applied, but we do not see a basis for creating new exemptions.

The third point I wanted to speak to concerns access to the NCIC, which is the criminal justice records system. We can see why this may be necessary as the FTC becomes more deeply involved in law enforcement matters, but because there was a recent decision to remove the data-quality obligation to ensure that the information in that database is accurate, we have some concerns now about opening it up to further use by the FTC, and even under provision in the draft bill that would allow the FTC to provide access to foreign law enforcement agencies, to this criminal justice system maintained in the United States.

Finally, Mr. Chairman, I just wanted to say, briefly, that we would like to see some new reporting requirements, so, as the FTC gets this new authority to investigate, you, the Committee Members, and the public have the ability to assess how well they are doing their job. And we would like to continue to urge the agency to focus also on privacy issues in the United States, because privacy protection continues to be a critical concern for American consumers.

So I would like to thank you very much for the opportunity to testify. I would be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC); ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today regarding consumer fraud and the reauthorization for the Federal Trade Commission. My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC). EPIC works with a wide range of consumer and civil liberties organizations both in the United States and around the world.

I would like to begin by thanking the Committee for focusing on the issue of cross-border fraud. One of the consequences of the rapid growth of the Internet has been the dramatic expansion of both commercial opportunity online and of commercial fraud. It is clearly in the interests of businesses and consumers to ensure a stable, growing, and fair online marketplace. Fraudulent and deceptive business practices that would otherwise be prosecuted in the United States should not be beyond the reach of United States law enforcement simply because an operator sets up shop outside the country. In similar fashion, government agencies seeking to protect the interests of consumers in their jurisdictions should expect the cooperation of the Federal Trade Commission when cross-border problems emerge.

I would also like to thank the FTC Chairman and the other members of the Commission for their efforts to address this new challenge and for the workshop in February that provided a wide range of important perspectives on this topic. Chairman Muris outlined the plan to pursue cross-border fraud in November of last year. He said that the FTC would advocate the adoption of a recommendation of the Organization for Economic Cooperation and Development (OECD) on cross-border fraud and would seek appropriate legislation. Commissioner Thompson, working through the International Marketing Supervision Network and in cooperation with the FTC's international counterparts, has helped develop a common understanding of what constitutes core consumer protection in the international realm.

The February workshop, organized by the FTC, set out the views of consumer and privacy organizations, businesses and foreign agency officials. Chairman Muris noted that cross-border complaints by U.S. consumers rose from 13,905 in 2001 to 24,313 in 2002. Canadian consumers also report a near doubling of complaints with online commerce between 2001 and 2002. The *Consumer Sentinel,* the FTC's central complaint database, records over 72 million dollars lost by U.S. consumers to cross-border fraud in 2002, nearly seventeen percent of all money lost to fraud. According to the FTC, 68 percent of all fraudulent foreign money offers come from companies located in Africa; 41 percent of fraudulent advance-fee loans come from Canadian companies, and 61 percent of fraudulent prize and sweepstakes offers are from companies located in Canada.

There was consensus at the February FTC workshop on the need to tackle the problem of cross-border fraud and to enable better cooperation between the FTC and its counterparts. The FTC proposal grows out of the work of the February meeting, the OECD, and the continued efforts to promote international cooperation.

EPIC has a particular interest in the protection of consumers in the global economy. We have successfully pursued privacy complaints on behalf of consumers under Section 5 of the FTC Act that have international implications. For example, our earlier work on the privacy implications of Microsoft Passport, the online authentication scheme, was considered favorably by both the Federal Trade Commission and the European Commission. EPIC also work closely with consumer and civil liberties organizations on the development of international policy. In particular, the Trans Atlantic Consumer Dialogue (TACD), a coalition of sixty consumer organizations in the United States and Europe, has urged officials on both sides of the Atlantic to address this challenge. Similar views have been expressed by consumer organizations in other parts of the world. We have also worked with the OECD for more than a decade, in areas such as privacy protection, consumer protection, cryptography, and electronic commerce, to promote the development of policies that promote economic growth and safeguard democratic values. We are pleased that these efforts have come together in the current proposal before the Committee to combat cross-border fraud.

In the statement today, I will recommend passage of legislation that will enable the Federal Trade Commission to work more closely with consumer protection agencies in other countries to safeguard the interests of consumers and users of new online services. Nevertheless, in creating these new enforcement authorities, there is

a clear need to safeguard important legal safeguards that are central to the U.S. form of government. In particular, certain provisions of the draft International Consumer Protection Enforcement Act, put forward by the FTC, should be revised to safeguard privacy, promote government accountability, and enable the development of reporting standards that will allow this Committee and the public to assess how well the FTC is doing its job and whether further steps may eventually be necessary. Without these changes, the legislation opens the door to abuse in that it creates new enforcement authority without corresponding safeguards. Civil liberties groups in both the United States and Europe have already expressed strong opposition to a proposal of this type that was put forward by the Council of Europe to combat cyber crime.

It is particularly important to understand that when the United States provides information about consumers and business in the United States to foreign law enforcement agencies it opens the door to prosecution that may not satisfy the substantive requirements or safeguard the procedural rights that would be available in this country.

Specific Provisions In The FTC Proposal

Information Disclosure to Foreign Governments (Sections 3 and 4)

We recognize that the cross border enforcement of consumer fraud will require cooperation between the FTC and sister agencies in other jurisdictions. To some extent, the sharing of information between agencies will be necessary to pursue violators and enforce judgments. At the same time, it is critical to ensure that only the necessary information is disclosed and that appropriate safeguards are established when such information is disclosed.

In our view, the FTC proposal creates too few restrictions on the disclosure of information concerning individuals and entities within the United States. One particular provision is simply offensive. A proposed amendment to Section 6 of the FTC Act that enables the FTC to assist foreign law enforcement agencies states that "such assistance may be provided without regard to whether the conduct identified in the request would also constitute a violation of the laws of the United States."

This provision further should be removed. We further recommend that the disclosure be only to "appropriate" foreign agencies, not "any" foreign agency as is currently specified in the bill, and we urge the FTC to post the names and contact information for any foreign agency that it considers appropriate to receive information. Not only should the FTC share information with appropriate agencies, it should share information only at appropriate times and in connection with a specific investigation. The Custom Service, for example, limits the exchange of information and documents with foreign customs and law enforcement to those instances where the Commissioner "reasonably believes the exchange of information is necessary. . ." 19 C.F.R. sect. 103.33. The FTC should not permit disclosures to any foreign government agency where the public and concerned parties cannot readily identify the agency.

We further recommend the recognition of a dual criminality provision to ensure that the United States assists in the prosecution of individuals and entities within the United States only in those circumstances where the crime charged would also be a crime under United States law. Absent such a provision, it is conceivable that a bookseller or music publisher in the United States could be subject to prosecution under foreign law where such government does not provide for strong protections for freedom of expression. This problem could arise in particular with publications that criticize state governments.

Amendments to U.S. Privacy Statues (Sections 6 and 7)

The FTC legislative proposal would amend two critical U.S. privacy statutes to reduce the likelihood that the target of an investigation would be notified of the investigation. In particular, the International Consumer Protection Enforcement Act would amend the Electronic Communications Privacy Act, and the Right to Financial Privacy Act. But the arguments for denying notice to the target of an investigation could too easily be made with respect to targets in the United States. The proposed changes here not only set a bad precedent but would also send a bad message to consumer protection agencies in other countries about the conduct of investigative actions by democratic governments.

We recommend that the provisions that reduce procedural safeguards be removed.

Disclosure of Financial Information (Section 8)

This provision would give the FTC authority to access financial bank reports and other financial data under the guise of fighting against cross-border consumer fraud and deception. However, there are no reporting or notification requirements that

record the exchange of information; there are no audit provisions that oversee the exchange of the information; there is no limit on who within the authorized agencies can exchange information, and there is no limit on what the content of the reports, records or other information shall consist off.

These provisions make it too easy for the listed agencies to share financial information. The provision would give the FTC discretion to share financial information without any oversight to make sure it is shared appropriately. This discretion leaves the exchange of information open to abuse. Moreover, there is no limit on what sort of information can be exchanged. There is no provision that states that records or information cannot consist of information identifiable to a particular customer. In this way, the authorized agencies could examine records about customers of financial institutions, without notification requirements, under the guise of examining records regarding the financial condition of the institution.

Although the objective of the proposed amendment, to ease the sharing of information amongst agencies involved in protecting consumers against fraud, is laudable, the amendment should include provisions that ensure that personal financial information is shared in an accountable and transparent manner. Acknowledging the FTC's desire to be able to share information appropriate to real-time law enforcement needs, the following additions to the amendment may be appropriate:

- a provision that information exchanged under 1112(e) cannot contain information identifiable to any one individual without triggering a reporting requirement.
- a provision that a designated official at the authorized agencies have a log of all personal information that is exchanged under 1112(e).
- a provision that such a log is available to the public under FOIA, unless there is a compelling law enforcement reason to exempt it.

Adding such provisions would allow an appropriate amount of accountability into the information exchange process, while still allowing the FTC and the other listed agencies to have the flexible use of information for their law enforcement needs.

Freedom of Information Act Exemptions (Sections 5 and 7)

The FTC proposes to exempt itself from certain open record obligations under the Freedom of Information Act. We believe this change is unnecessary and, if enacted, will reduce government accountability.

The current FOIA exemptions for ongoing criminal investigation, § 552(b)(7)(A), and for the protection of confidential sources, (b)(7)(D), would likely prevent the disclosure of information that the FTC seeks to protect without any further amendment. Moreover, three other exemptions may also apply to information collected by the Commission; the exemption for business information under § 552(b)(4); for personal privacy under § 552(b)(6); and for records of financial institutions under § 552(b)(8).

EPIC has already pursued an extensive FOIA request with the FTC involving the investigation of privacy complaints under Section 5 of the FTC Act. In that case, the FTC has demonstrated its willingness to apply the current statutory exemptions. Some of the information we sought concerning current matters was withheld. The FTC cited the (b)(7)(A) exemption.

Since the existing exemptions already provide adequate protection for the Commission, a new exemption is not necessary and only adds confusion to a long-standing statutory scheme that has been subject to judicial interpretation for almost thirty years. Therefore, we recommend that provisions to limit the application of the Freedom of Information Act be stricken from the FTC proposal, or at the least that a thorough analysis be done to determine whether the current exemptions combined with current case law are sufficient before any new exemption is created.

Access to Criminal Justice Records (Section 12)

Section 12 of the proposed Act would grant the FTC access to the National Crime Information Center, the Nation's most extensive computerized criminal history database, following an agreement with the Attorney General to (A) establish the scope and conditions of the FTC's access to the database, and (B) establish the conditions for the use of the data. Section 12 would further permit the FTC to disclose NCIC data to foreign law enforcement agencies pursuant to procedures that require at least prior certification that such information will be maintained in confidence and will be used only for official law enforcement purposes.

While we recognize the interest that the FTC may have in accessing the NCIC record systems, there are three problems with this proposal. First, it was never anticipated that the FTC would have access to this record system and it was also never anticipated that the FTC could allow foreign law enforcement agencies access

to this record system. This is precisely the type of mission creep that results from the creation of criminal justice databases lacking adequate statutory constraints that civil liberties groups on both the right and the left have opposed.

Second, this proposal to expand access to the NCIC follows just a few months after a decision by the FBI to exempt itself from the data quality obligations that would otherwise apply to this system of records under the 1974 Privacy Act. More than 90 organizations and 5,000 individuals across the United States expressed their opposition to this decision by the Bureau. The lack of data quality obligations for the NCIC increases the likelihood that individuals will be wrongly stopped and detained, perhaps even placed in dangerous law enforcement interdictions, because of errors in the most important criminal history record system in the United States that the Department of Justice no longer feels obliged to keep accurate. The further expansion of NCIC use, while this issue remains unresolved, should be postponed until the data accuracy obligation is restored.

Finally, it is important to note, particularly in the context of transborder data flows that the NCIC record system does not meet all of the international standards for privacy protection. Most significantly, the proposal does not provide for access by the record subject to inspect and correct records concerning the individual. Further amendments may be necessary to enable first party access to NCIC records.

We recommend against providing the FTC with access to the NCIC until the data quality obligation is restored and some right of first party access to the record system is established. In the alternative, we would recommend revisions to the proposed bill that would add a new provision that would require the FTC to "establish with a high degree of confidence that the data obtained by the FTC from the NCIC is accurate." We further recommend that section 12 more accurately specify the purposes for which the FTC may use NCIC data. In particular, the FTC should be required to show that evidence gathered from the NCIC would likely reveal that the data subject has previously committed an act that would fall within the FTC's jurisdiction or that the data subject may have moved assets across national borders to avoid prosecution.

General Recommendations

Reporting

We recommend the creation of new reporting requirements that would focus specifically on the FTC's activities undertaken pursuant to this new legislative authority. There should be an annual report provided to the Congress and made available to the public at the website of the FTC. This report should include such information as the number of complaints received during the past year, the number of investigations pursued, and the outcome of these investigations including whether any damages were assessed and whether any relief was provided to consumers as a result of the investigation. The report should also indicate which foreign agencies the FTC cooperated with and the nature of the information provided and the information received.

The FTC has already begun the process of making some of this information available with the Consumer Sentinel website. Canada, Australia and the United States, have also established eConsumer project that helps provide similar information on the international front. While both projects are important, we believe that formalizing reporting requirements for investigations as well as complains will make it easier to assess how well the FTC and other agencies are responding to the challenges of cross-border fraud.

We would also urge the FTC to consider the creation of an advisory council for the major multilateral law enforcement groups, such as the International Consumer Protection and Enforcement Network, that would allow the participation for a U.S. consumer representative and a U.S. business representative. Participation by representatives of the consumer and business community will help ensure oversight and reduce the risk of unaccountable activities.

International Privacy Framework

The OECD proposal for protecting consumers in the global economy is consistent with other efforts of the OECD to promote economic growth while safeguarding democratic values. In this spirit, we would like to underscore the need to ensure that new efforts undertaken by the United States in cooperation with other governments should be consistent also with the OECD recommendation on privacy protection. The FTC has already worked to ensure that principles similar to those contained in the OECD Privacy Guidelines were established for transborder data flows between the United States and Europe in the context of the Safe Harbor proposal. That arrangement allows U.S. firms to enter European markets and process data

on European consumers on the condition that they follow and enforce strong privacy standards.

We urge the adoption of a similar framework to regulate the transfer and use of personal information that will occur between national governments as they pursue joint investigations and prosecutions. Governments, no less than the private sector, should be held to high standards in their use of personal information, particularly because the misuse of such information may subject individuals to unfair and unfounded prosecutions.

Continued Focus in Privacy Issues in the United States

Even as the Federal Trade Commission pursues its efforts to address the challenge of crossborder fraud, it is important not to lose sight of the important work that must still be done in the United States to safeguard the interests of consumers. We commend the Commission for its leadership in the creation of a national telemarketing "Do-Not-Call" list, and for its victories for consumer privacy in the two Trans Union cases upholding protections in the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act.

However, as the top consumer watchdog in the government, the Commission must continue to set a high standard to protect individuals' privacy. The Commission only recognizes four Fair Information Practices (notice, choice, access, security) to evaluate individuals' privacy rights. This falls short of the standard set by the Privacy Act of 1974, which recognizes additional rights including use limitations, data destruction, and rights of correction. Internationally, consumer protection watchdogs have adopted eight Fair Information Practices (collection limitation, data quality, purpose specification, use limitations, security, openness, individual participation, and accountability) in order to establish rights and responsibilities in the use of individuals' data.

We believe the Commission should endorse best practices for Internet mailing lists and support the opt-in approach. This will have a significant impact in the efforts to reduce spam, or unsolicited commercial e-mail. We also note that the Commission has failed to endorse strong consumer safeguards for the Fair Credit Reporting Act, which is a critical consumer statute now under review by the Congress. Strong leadership on the FCRA is important for the mission of the FTC.

Furthermore, the Commission should begin to consider new technologies that have significant privacy implications for consumers in the marketplace. For instance, RFID, or "Radio Frequency Identification" chips may enable tracking of individuals in the physical world the same way that cookies do on the Internet. This week Microsoft announced that it plans to support RFID applications in future versions of its software. It would be appropriate for the FTC to begin the process of exploring how these new tracking techniques may affect consumer confidence and whether new safeguards may be required.

Conclusion

There is a clear need to enable the Federal Trade Commission to work in cooperation with consumer protection agencies in other countries to investigate and prosecute cross-border fraud and deceptive marketing practices. New legislation will be necessary to accomplish the goal. Nevertheless, the bill should be drafted in such a way so as to safeguard important American values, including procedural fairness, privacy protection, and open government. These principles of good government will assist consumer protection agencies around the world combat cyber fraud, and will help strengthen democratic institutions.

References

Statement of Cedric Laurant, EPIC Policy Counsel, on "Potential Partnerships among Consumer Protection Enforcement Agencies and ISPs and Web Hosting Companies" for the Public Workshop on Public/Private Partnerships to Combat Cross-Border Fraud, before the Federal Trade Commission (February 19, 2003)

EPIC, "Joint Letter and Online Petition: Require Accuracy for Nation's Largest Criminal Justice Database"

Federal Trade Commission, Consumer Sentinel, Cross-Border Fraud Trends, January—December 2002, (February 19, 2003)

Federal Trade Commission, Budget Summary, Fiscal Year 2004, Congressional Justification

Federal Trade Commission, Budget Summary, Fiscal Year 2003, Congressional Justification

Federal Trade Commission, Consumer Sentinel website

Federal Trade Commission, Cross Border Fraud website

Federal Trade Commission, "FTC Chairman Muris Presents the FTC's New Five-Point Plan for Attacking Cross-Border Fraud and Highlights Links Between Competition and Consumer Protection" (October 31, 2002)

In the Matter of Microsoft Corporation, No. 012–3240, before the Federal Trade Commission

International Consumer Protection Enforcement Act of 2003, draft, May 21, 2003

Organization for Economic Cooperation and Development (OECD), Directorate for Science, Technology and Industry, Committee on Consumer Policy, "Cross-Border Co-operation in Combating Cross-Border Fraud: The US/Canadian Experience." (February 6, 2001)

Organization for Economic Cooperation and Development (OECD), Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"), reprinted in Marc Rotenberg, ed., *Privacy Law Sourcebook: United States Law, International and Recent Developments* 324–352 (EPIC 2002)

Transatlantic Consumer Dialogue, "Resolution on Protecting Consumers from Fraud and Serious Deception Across Borders," Doc No. Internet-28–02 (November 2002)

About Epic

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and to promote the Public Voice in decisions concerning the future of the Internet. More information is available online at *www.epic.org.*

Senator SMITH. Thank you, Mr. Rotenberg.

Ms. Grant.

STATEMENT OF SUSAN GRANT, DIRECTOR, NATIONAL FRAUD INFORMATION/INTERNET FRAUD WATCH, NATIONAL CONSUMERS LEAGUE

Ms. GRANT. Thank you for inviting the National Consumers League, America's pioneer consumer organization, to testify today. I am going to focus specifically about cross-border fraud, but I would be happy to answer questions about spam or privacy, in general.

We know about fraud, because we hear about it directly every day. Since 1992, we have operated a telemarketing fraud hotline for consumers to get advice and report suspected fraud. And in 1996, we expanded that service to cover Internet fraud. We do not just hear from consumers. Businesses are also targeted for a variety of scams.

The information that we get from victims of telemarketing and Internet fraud is transmitted quickly and automatically to law enforcement agencies in the U.S. and Canada. We also upload that information, on a weekly basis, to the FTC's Consumer Sentinel Database.

As the FTC pointed out earlier, the marketplace has become more global, and so has telemarketing and Internet fraud. In 1995, only about 5 percent of the telemarketing-fraud complaints we received involved companies in other countries. In 2002, that was nearly 17 percent. In 1997, foreign companies represented about 6 percent of the Internet-fraud complaints that we received. In 2002, it was nearly 15 percent. And I think it is fair to say that these numbers understate the problem, since, in many instances, consumers may think that companies are in the U.S., when, in fact, through call forwarding, mail forwarding, and other ways of fooling them, the con artists are really in other countries. Internet and E-mail can also mask the true identity and location of con artists.

In addition, the growing use of electronic-payment systems makes it easy for crooks to pick consumers' pockets across the border. As a result, financial institutions and others also suffer financial harm from these scams.

One example of a typical fraud complaint that we receive, of a cross-border nature, a New York man received a telemarketing call offering him a credit card with $1,000 credit limit if he paid an upfront fee of $198. And these scams are often targeted at people who are having financial problems and difficulty getting credit cards. He agreed. He gave his bank account number for the fee to be debited. He did not get a credit card. These people never do. He got a list of card insurers who he could contact directly, with whom this company, I am sure, has no relation. And this is information that a consumer could easily get by going on the Internet or going to the library. And it appears that the company is based in Barbados.

Victims of fraud expect Governments to help them and stop bad actors from robbing others. They do not understand that there will be any impediment to helping them, simply because a company turns out to be located across the border.

And we all want people to be more confident when they shop by telephone and online. We want them to be able to take advantage of this global marketplace to buy goods or services from abroad, and also consumers in other countries to buy goods and services from legitimate business here in the U.S. And consumer organizations everywhere have these same concerns.

Last year, the Transatlantic Consumer Dialogue, a coalition of U.S. and European Union member-country consumer organizations, adopted a resolution supporting the OECD guidelines to improve enforcement against cross-border fraud and deception. The U.S. is leading that effort, and now it wants to put words into action by asking Congress to remove unnecessary barriers to sharing information about fraud and deception with agencies in other countries, providing mutual assistance to bring legal actions against cross-border fraud, and get restitution for victims, make it easier to get information about cross-border fraud and deception from the private sector, who often hears about it first, and give the FTC more flexibility and resources to pursue con artists wherever they are. And we are confident that this can be done with appropriate safeguards for privacy and due process.

Thank you.

[The prepared statement of Ms. Grant follows:]

PREPARED STATEMENT OF SUSAN GRANT, DIRECTOR, NATIONAL FRAUD INFORMATION CENTER/INTERNET FRAUD WATCH, NATIONAL CONSUMERS LEAGUE

Thank you very much for inviting me to comment on this important legislation. The National Consumers League (NCL) is a nonprofit organization that was founded in 1899 to protect and advance the economic and social interests of consumers and workers. In the early days of NCL's history, there was no telemarketing or Internet fraud, but there were unscrupulous people promoting bogus investment opportunities, miracle cures, pyramid schemes, phony games of chance, and other types of fraud through newspaper ads, the mail, door-to-door, and other marketing methods of the day.

Since then, new marketing channels such as telemarketing and the Internet have been developed. Not surprisingly, con artists have seized on them to widen their reach. Because these scam operators are often in one location and their victims are

in others, it is very confusing for consumers to know whom to contact to ask questions or seek help. That's why in 1992 NCL created the first nationwide toll-free hotline to offer consumers advice about telemarketing solicitations and notify law enforcement agencies quickly about fraudulent telemarketers. In 1996 the Internet fraud component was added to our system.

Consumers can call 800–876–7060 to speak to a live counselor or go to *www.fraud.org.* The website has tips about the most common types of telemarketing and Internet scams, a special section on fraud against seniors, fraud statistics, and a complaint form. Consumers can report suspected telemarketing and Internet fraud by telephone or online. That information is automatically transmitted electronically to the appropriate agencies among more than 200 local, state and Federal agencies in our system from the United States and Canada, alerting them to scam operators that may merit investigation and victims that need their help. It is also uploaded on a weekly basis to the Federal Trade Commission's Consumer Sentinel database for use by law enforcement agencies.

As the marketplace has become more global, so has telemarketing and Internet fraud. In 1995, only about 5 percent of the telemarketing fraud complaints we received concerned companies in other countries; by 2002 foreign companies accounted for nearly 17 percent of our telemarketing fraud complaints. In 1997, the first full year of our Internet Fraud Watch program, about 6 percent of complaints involved foreign companies; by 2002 it was nearly 15 percent. These statistics probably understate the problem, since in many cases consumers may not be sure where the fraudulent operators are located. Call forwarding, mail drops, and the growing use of electronic payment systems that negate the need to send checks or money orders to vendors make knowing where they actually are very difficult. The Internet and e-mail can also mask the sellers' true identities and locations.

Consumers lose millions of dollars to cross-border scams every year. Businesses are negatively impacted as well. Many telemarketing and Internet frauds are targeted specifically at business victims. Financial institutions and others also suffer damages as a result of disputed credit card charges or debits for fraudulent transactions, nonpayment for services provided to fraudulent vendors, and general loss of consumer confidence.

Here is an example of a typical cross-border complaint from our hotline. Michael M. from Brooklyn, New York received a telemarketing call offering him a credit card with a $1,000 line of credit for an upfront fee of $198. We don't know his particular financial situation, but these types of scams are often targeted to people who are having credit problems. He agreed and gave his bank account number for the fee to be debited. He didn't get a credit card. What he received was four sheets of paper listing banks that offer credit cards—information that is available free from the local library or on the Internet. The company appears to be in Barbados.

We don't know if this man realized where the company was located, but even when consumers are aware that they are dealing with vendors in other countries, that fact may not discourage them from making purchases—nor should it. We want consumers to feel confident about taking advantage of the global marketplace, whether they are U.S. consumers interested in goods or services from abroad, or consumers in other countries who want to do business with companies here.

We know from our direct contact with fraud victims that most don't understand that recourse will probably be more difficult, perhaps impossible, if the culprits are in other countries. They want and expect their government to help them. They don't think it's fair that fraudulent operators may be able to get away with it simply because they're across the border. It's not only U.S. consumers who want to shop with confidence and expect their governments to stop the bad actors in the marketplace—consumers in other countries have the same expectations.

Last year, the Trans Atlantic Consumer Dialogue, a coalition of consumer organizations from the U.S. and European Union countries, adopted a resolution supporting the efforts by the Organization for Economic Cooperation and Development to craft guidelines for improving enforcement against cross-border fraud and deception. That document can be found at *http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=179*.

The U.S. and the Federal Trade Commission in particular, has led the work on these forward-looking guidelines. Now the U.S. is leading again by putting words into action, asking Congress to: remove unnecessary barriers to sharing information about fraud and deception with law enforcement agencies in other countries; provide for assistance in bringing cross-border legal actions; make it easier to obtain information about suspected con artists from the private sector; and give the Federal Trade Commission more flexibility and resources to pursue con artists wherever they are.

We believe that these changes are absolutely necessary to protect consumers and legitimate businesses in the marketplace of the 21rst century. We are confident that Congress and the Federal Trade Commission can agree on legislation that will give law enforcement agencies the tools they need to combat cross-border fraud and deception more effectively, with the appropriate safeguards for privacy and due process.

Thank you very much for giving us the opportunity to share our views on this matter. We will be happy to provide you with any additional information you may need.

Senator SMITH. Thank you.
Ms. Deutsch.

STATEMENT OF SARAH DEUTSCH, VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL, VERIZON COMMUNICATIONS

Ms. DEUTSCH. Thank you, Mr. Chairman and Members of the Committee, for the opportunity to testify on the issue of cross-border fraud.

The issue of cross-border fraud is a serious and growing problem. We were pleased to participate in the FTC's Public-Private Partnership Workshop to combat cross-border fraud, this past February. And Verizon has had considerable experience working with law enforcement to fight Internet fraud and to protect our customers and the public.

As an Internet service provider, we have most commonly encountered credit-card fraud schemes, a host of Nigerian fraud scams, and, of course, a huge amount of spam, including E-mail that fraudulently contains spoof domain names, including domain names originating falsely from Verizon.

We have carefully studied the proposed draft legislation to expand the FTC's authority in assisting foreign law-enforcement agencies. We also support that effort and offer, today, a few suggestions on how to strengthen such legislation.

Verizon believes that one critical missing prerequisite in the proposed legislation is a concept called "dual illegality." Before the FTC conducts investigations or assists in enforcement for any foreign counterpart, the underlying activity must, at a minimum, be considered illegal in both the foreign country requesting assistance and in the United States. For example, in many European countries, advertising laws prohibit activities such as comparative advertising, money-back guarantees, such as that offered by the Land's End catalog, sales promotions, giveaways, or advertising particular professions, such as medicine or law. The global reach of content on the Internet means that legal activity originating from one country can result in potential liability in another.

In Australia, Dow Jones was successfully sued for defamation, because the Website it hosted in New Jersey contained an article that an Australian citizen found offensive. Yahoo! was found liable in France for auctioning items, on its U.S. auctionsite, that were considered illegal in France, yet protected here at home under the First Amendment.

So common sense dictates that U.S. taxpayer dollars should not be spent investigating legal activities that could later be used by foreign governments to harm U.S. companies.

The FTC should also validate the authenticity of a request coming from a foreign government to ensure that it originates from a

legitimate foreign counterpart to the FTC. Section (2) of the proposed bill broadly defines a foreign law enforcement agency to include multinational organizations and even private organizations that can be vested with authority by undefined political subdivisions of a foreign state. In order to prevent the resources of the FTC and other parties from being diverted or diluted, we believe that a foreign law enforcement agency should be narrowly defined as "the foreign legal equivalent of the FTC."

Verizon looks forward to cooperating with the FTC, in its role as a civil-enforcement agency, in investigations under the Electronic Communications Privacy Act, in the same manner that we assist criminal law enforcement agencies today. We are concerned that Section (6)(d), of the proposed legislation would allow the FTC to obtain, using its own administrative subpoena, the text of E-mail messages without prior notice to the subscriber, as currently required under Section 2703 of ECPA. This provision is inconsistent with other provisions in ECPA that prohibit any governmental agency to obtain this same information without notice to the customer in the absence of a judicially ordered search warrant.

As you may know, Verizon is currently defending the due process and privacy rights of our Internet subscribers in a highly publicized copyright lawsuit that also involves the issue of when a judge must issue a subpoena. The RIAA sued Verizon, arguing that any private party claiming to be a copyright owner should be entitled to obtain an Internet users identity for activity not occurring on our system or network by filing a one- page form with the clerk of a court, rather than first filing a lawsuit and obtaining a subpoena from a judge or magistrate. And although Verizon does not support piracy in any way, we believe that this overly broad process will result in instances of consumer fraud, way beyond piracy issues, and ultimately wind up on the FTC's doorstep.

So we are looking to Congress to offer a legislative fix to the RIAA case, and hope that the FTC inconsistency will be worked out so they operate under the same rules as other law enforcement agencies.

Finally, third parties who cooperate in good faith with the FTC in its cross-border fraud investigations should enjoy a broad exemption against viability in the statute and should be entitled to reimbursement of the provider's cost. Providers are currently reimbursed for their costs under ECPA and other statutes, and should be similarly compensated under this bill.

Thank you for the opportunity to testify, and Verizon looks forward to working with the Committee and the FTC on these important issues.

[The prepared statement of Ms. Deutsch follows:]

PREPARED STATEMENT OF SARAH DEUTSCH, VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL, VERIZON COMMUNICATIONS

Thank you Mr. Chairman and members of the Committee for the opportunity to testify on the issue of cross-border fraud contained in the proposed Federal Trade Commission reauthorization legislation. Verizon Communications is one of the world's leading providers of wireline and wireless communications in the United States. Verizon also has a significant presence in over 30 countries in the Americas, Europe, Asia and the Pacific.

The issue of cross-border fraud is a serious and growing problem. Verizon was pleased to participate this past February in the FTC's Public/Private Partnership Workshop to combat cross-border fraud. Verizon has had considerable experience working with law enforcement to fight Internet fraud and to protect our customers and the public. Internet fraud harms innocent consumers and communications providers. If not addressed, Internet fraud ultimately undermines consumers' confidence in the Internet as secure medium through which to communicate and do business. As an Internet service provider, we have most commonly encountered credit card fraud schemes, a host of Nigerian fraud scams, and of course, a huge amount of unsolicited commercial email or spam, including email that fraudulently contains "spoofed" domain names falsely addressed as originating from Verizon or another service provider.

We have carefully studied the proposed legislation to expand the FTC's authority in assisting foreign law enforcement agencies in investigating or enforcing fraudulent, deceptive or unfair commercial practices. We offer today a few suggestions on how to strengthen such legislation. As an initial matter, however, we believe this particular legislation would be more effective if it was introduced together with an international agreement that binds foreign governments to provide mutually corresponding assistance to the United States. A cross-border fraud treaty, for example, could better clarify all signatories' obligations to provide mutual legal assistance, create ground rules on what is considered a "fraud," set certain financial thresholds for the investigation of such frauds and clarify the roles and obligations of the parties.

Verizon believes that one critical, missing prerequisite in the proposed legislation is a concept called "dual illegality." Before the FTC conducts investigations or assists in enforcement for any foreign counterpart, the underlying activity must, at a minimum, be considered illegal in both the foreign country requesting assistance and in the United States. Section 4 of the proposed legislation, however, permits the FTC to provide assistance to foreign law enforcement agencies even if the underlying conduct is considered legal in the United States. U.S. companies could be the targets of unintended consequences if the concept of "dual illegality" is not included in this legislation. For example, in many European countries, advertising laws prohibit activities such as comparative advertising, money-back guarantees (like that offered by the Lands End catalog), sales promotions, giveaways or advertising particular professions such as medicine or law. In France, a directory provider was found liable for misleading advertising by inadvertently depicting the wrong brand in a line drawing of a product for sale in its customer's advertisement.

The global reach of content on the Internet means that legal activity originating from one country can result in liability in another. Foreign courts have recently issued a number of troubling international jurisdictional decisions affecting U.S. companies. Many of these countries have tried to impose liability on U.S. companies simply because the Internet sites they hosted in the United States contained information that was "accessible" in another country. For example, in Australia, Dow Jones was successfully sued for defamation because a website it hosted in New Jersey contained an article that an Australian citizen found offensive. Yahoo was found liable in France for auctioning items on its U.S. auction site that were considered illegal in France yet protected under the First Amendment here at home. Common sense dictates that U.S. taxpayer dollars should not be spent investigating legal activities that could be later used by foreign governments to harm U.S. companies. The FTC, as the gatekeeper through which requests for foreign assistance are channeled, should be conducting an initial substantive review of each request to make sure that the underlying activity is first considered illegal in the U.S.

The FTC should also validate the authenticity of a request for foreign assistance to ensure that it originates from a legitimate foreign counterpart to the FTC. We believe that the proposed legislation should better define which entities qualify as a "Foreign Law Enforcement Agency." Section 2 of the proposed bill broadly defines a foreign law enforcement agency to include multinational organizations and even private organizations that can be vested with authority by undefined "political subdivisions" of a foreign state. "Private organizations" might include (1) foreign collecting societies, who currently seek to extort levies from U.S. companies in Canada for the protected act of Internet "caching"; or (2) the EU, which has proposed a controversial new "IPR enforcement directive," which could subject U.S. companies to broad injunctions and monetary damages. In order to prevent the resources of the FTC and others parties from being diverted or diluted by numerous entities seeking assistance, a "Foreign Law Enforcement Agency" should be narrowly defined as the foreign legal equivalent of the FTC. This should include only those agencies that serve as an official instrumentality of the state for the specific purpose of engaging in consumer protection. Verizon has reservations about extending the obligation of

the FTC to assist ambiguously defined “multinational organizations.” Qualifying multinational organizations should therefore be limited to those organizations whose primary purpose is to protect consumers against fraud and are explicitly authorized by their member states’ law enforcement agencies to do so.

Verizon looks forward to cooperating with the FTC, in its role as a civil enforcement agency, in investigations under the Electronic Communications Privacy Act in the same manner that we assist criminal law enforcement agencies today. We are concerned that Section 6(d) of the proposed legislation would allow the FTC to obtain, using its own administrative subpoena, the text of email messages (or “stored communications”) without prior notice to the subscriber or customer, as currently required by Section 2703(b)(1)(B). This provision is inconsistent with the preceding provision in ECPA (Section 2703(b)(1)((A)), which does not permit criminal law enforcement agencies (or any other “governmental entity”) to obtain this same information *without notice to the customer* in the absence of a *judicially-ordered* search warrant. There is no reason why the FTC should operate under different rules than that required for other law enforcement agencies. As you may know, Verizon is currently defending the due process and privacy rights of our Internet subscribers in a highly publicized copyright lawsuit currently on an expedited appeal to the DC Circuit Court of Appeals. This case also involves the issue of when a judge must issue a subpoena. The RIAA sued Verizon arguing that any private party claiming to be a copyright owner should be entitled to the right to obtain an Internet user’s identity without first filing a lawsuit in court or obtaining a subpoena from a judge or magistrate. RIAA argues that anyone who makes a mere allegation of infringement can obtain a subpoena, not from a real judge or magistrate, but from the clerk of a court, who has no discretion but to stamp a one page form. The fallout from RIAA case, if not overturned on appeal, is that any person armed with a user’s Internet Protocol (“IP”) has an unprecedented shortcut to learn any consumer’s name, address and phone number without notice to the subscriber. This process will certainly result in instances of consumer fraud and privacy abuses, and many complaints will ultimately wind up on the FTC’s doorstep. We are looking to Congress to offer a legislative fix to the RIAA case before consumers suffer from misuses of this process. With respect to this provision in the FTC legislation, we would strongly urge amending the legislation to first require, if not a search warrant, at the very least, an order issued by a judge before granting the FTC, alone of all governmental entities, unprecedented new rights to obtain the contents of email communications without prior notice to the subscriber.

Finally, third parties who cooperate in good faith with the FTC in its cross-border fraud investigations should enjoy a broad exemption against liability. Section 2703(e) of ECPA, for example, broadly exempts providers from liability for providing information, facilities, or assistance to law enforcement. Section 6(e) of the proposed legislation could be misread as providing an exemption only when a person has either provided information to the FTC or failed to provide notice to another. Parties cooperating in good faith with the FTC should benefit from the same broad exemption from liability whether they provide assistance to a civil or criminal law enforcement agency. We would also recommend that the legislation include specific language providing for reimbursement of the provider’s costs in assisting the FTC in its investigations on behalf of foreign governments. Providers are currently reimbursed for their costs under ECPA (and other statutes) and should be similarly compensated under this bill.

Thank you for the opportunity to testify today. Verizon looks forward to working with the Committee and the FTC on this important issue.

Senator SMITH. Thank you, Ms. Deutsch.

Regrettably, another vote has been called. I just wonder if our remaining witnesses—if you have, sort of, a summation of your testimony, we may be able to get it all completed before this vote.

So, Mr. Sarjeant, your full testimony will be included in the record, but I do not know if you—I do not want to shortchange your time here, either.

STATEMENT OF LAWRENCE E. SARJEANT, VICE PRESIDENT LAW AND GENERAL COUNSEL, UNITED STATES TELECOM ASSOCIATION (USTA)

Mr. SARJEANT. Well, thank you, Mr. Chairman, and I will try and compress it as much as I can.

I want to try and focus on the point—the FTC's request for concurrent jurisdiction over common carriers with the FCC. And I just—I will take my limited time to focus on what I believe the FCC is doing to demonstrate that there is no gap.

Ever since the Congress gave the FTC consumer-protection jurisdiction, it recognized that the FTC should not duplicate the authority of other Federal agencies. That is why several industries are exempt from the FTC's otherwise broad Section 5 authority.

The exemption in Section 5 of the Federal Trade Commission Act is not limited to telecommunications common carriers. It currently extends to banks, savings and loans institutions, air carriers, persons subject to the Packers and Stockyards Act of 1921, and other common carriers subject to the acts to regulate commerce. These are all industries subject to less pervasive regulation than telecommunication's industry providers, particularly incumbent local exchange providers, who, under the 1996 act, are subject to unprecedented obligations to unbundle their networks and share those networks with other providers.

Three years ago, the FCC established an enforcement bureau to focus resources on compliance with the Communications Act in implementing regulations. The enforcement bureau enforces FCC rules, orders, and license authorizations. This bureau has a telecommunications consumers division, which investigates the practices of carriers that affect consumers. It also resolves formal complaints brought by consumers and establishes guidelines for companies in areas such as advertising.

The FCC also has a Consumer and Governmental Affairs Bureau. Among other things, this bureau distributes information to enable consumers to make wise choices in finding the best rates for telecommunications products and services. It conducts consumer-related rulemakings, handles informal wireless and wireline carrier billing and service complaints, and provides assistance to people with hearing, visual, speech, and other disabilities to allow their participation in FCC actions and ensure their opportunity to communicate.

Since November 1999, the FCC has issued proposed forfeitures, fines, and entered into consent decrees amounting to over $17 million for slamming violations. It has proposed a $5.4 million fine against the company for telephone Consumer Protection Act violations.

The FCC's enforcement bureau entered into a consent decree with three common carriers for failing to provide required consumer information that resulted in total contributions of $311,000. Just since March of this year, FCC enforcement activities have generated more than $15 million in fines and contributions. Section 201 of the Communications Act gives the FCC the authority to ensure that the practices of common carriers, in connection with the provision of communications services, are just and reasonable. The FCC has addressed areas such as consumer privacy, slamming, the regulation of practices of operator service providers and aggregators, truth in billing for common carriers in order to reduce slamming, and other telecommunications fraud.

The FCC, on the basis of authority conferred by Congress, has already fully occupied the field, when it comes to the practices of

interstate telecommunication's common carriers. With respect to intrastate carriers, the States continue to have full authority to regulate carrier practices affecting consumers and competitors, pursuant to existing laws.

USTA believes that the FCC has demonstrated a commitment to enhancing its enforcement efforts, and it has held carriers and others within its jurisdiction accountable when they have violated laws or FCC regulations. When the FCC has concluded it lacks jurisdiction to take enforcement, it has deferred to the FTC. The FCC has referred over 2,000 complaints to the FTC for disposition concerning the unauthorized placement of non-common-carrier charges on telephone bills, or as to other matters over which it has no jurisdiction.

In summation, Mr. Chairman, we see no gaps, and we see no need for concurrent jurisdiction. Concurrent jurisdiction would only add to confusion and duplication. And we ask the Committee to not consider the extension of concurrent jurisdiction for the FTC over common carriers.

[The prepared statement of Mr. Sarjeant follows:]

PREPARED STATEMENT OF LAWRENCE E. SARJEANT, VICE PRESIDENT LAW AND GENERAL COUNSEL, UNITED STATES TELECOM ASSOCIATION (USTA)

Thank you Mr. Chairman and members of the Committee for giving the United States Telecom Association (USTA) the opportunity to testify and present its views on The Federal Trade Commission Reauthorization Act and the question and issues concerning whether the Federal Trade Commission (FTC) should be authorized by Congress to have concurrent jurisdiction with the Federal Communications Commission (FCC) over telecommunications common carriers (hereafter "carriers"). I am Lawrence E. Sarjeant, and I serve as Vice President Law and General Counsel of USTA. I appear at the hearing today on behalf of the entire association. USTA is the nation's oldest trade organization for the local telephone industry. USTA's carrier members provide a full array of voice, data and video services over wireline and wireless networks.

I testified before this Committee on July 17, 2002, regarding this very same jurisdictional issue. In that testimony, I advised the Committee of USTA's strong objections to the Congress providing the FTC with jurisdiction over carriers. USTA's views have not changed. It remains in strong opposition to granting the FTC concurrent jurisdiction with the FCC for the regulation of carriers.

A. The FCC and the States Already Subject Carriers to Comprehensive Regulation

USTA is not opposed to regulatory accountability for carriers that have breached the public's trust and engaged in unjust, unreasonable or deceptive conduct. USTA is opposed to adding another regulatory agency and another regulatory regime to manage the telecommunications industry. The telecommunications industry, especially those carriers classified under the Telecommunications Act of 1996 (1996 Act) as incumbent local exchange carriers (ILECs) already operate under close scrutiny by federal and state regulators. ILECs are pervasively regulated. Notwithstanding Congress' 1996 Act policy goal of fostering a deregulatory environment, ILECs are more regulated today than at anytime in history, including when they were uniformly considered to be natural monopolies by antitrust and telecommunications policymakers.

The FTC since its creation in 1914 has *not* regulated carriers. There is a statutory exemption for "common carriers" from FTC regulatory authority that has been recognized by the federal judiciary (*See, e.g., FTC* v. *Miller,* 549 F.2d. 452, 7th Cir, 1977) and that has been reaffirmed by the Congress. The reason for the exemption has been and is now the same. There is no absence of regulation—there is no regulatory void to fill. Common carriers, including telephone common carriers, were in 1914 subject to regulation by the Interstate Commerce Commission, and upon creation of the FCC by Congress in 1934, the regulatory authority over telephone common carriers was transferred to it. The exemption from FTC regulatory authority was continued.

B. The FCC Has Used Its Statutory Authority to Protect Consumers

The FCC has determined that Section 201(b) of the Communications Act of 1934, as amended (Communications Act) "requires that common carriers'" "*practices* . . . for and in connection with . . . communication service, shall be just and reasonable and any such . . . *practice* . . . that is unjust or unreasonable is hereby declared to be unlawful . . ." (FCC–FTC Joint Policy Statement, FCC 00–72, 2/29/2000, para. 4).

The Congress has given the FCC specific statutory to address telemarketing practices and unsolicited faxes in the *Telecommunications Consumer Protection Act* (TCPA). The TCPA has been codified at Section 227 of the Communications Act. Additionally, the FCC has statutory authority to: address unauthorized changes of customers' carriers (slamming) (Communications Act at Section 258); protect the privacy of customer information (Communications Act at Section 222); and regulate certain business practices of operator services providers and aggregators (Communications Act at Section 226). The FCC has implemented *Truth in Billing Requirements for Common Carriers* in order "to reduce slamming and other telecommunications fraud" and "to aid customers in understanding their telecommunications bills, and to provide them with the tools they need to make informed choices in the market for telecommunications services." (47 C.F.R. § 64.2400 *et seq.*)

Just this year, the Congress passed the *Do Not Call Implementation Act* (DNCA/ P.L. 108–10), which President Bush signed into law on March 11,2003. The DNCA directs the FCC to issue, within 180 days from the date of the DNCA enactment, a final rule pursuant to a rulemaking proceeding that it had already commenced under its TCPA authority in order to revise its rules on telemarketing and unsolicited faxes. The FCC was also required by the DNCA to coordinate with the FTC to "maximize consistency" with the FTC's Do Not Call Rule.

The Report (H.R. Rep. 108–8, 108th Cong., 2003) that the House Committee on Energy and Commerce filed with respect to H.R. 395, which bill ultimately became the DNCA addressed this jurisdictional issue in two instances. First, it reaffirmed that the FTC ". . . does not have jurisdiction over common carriers (such as telecommunications companies and airlines) ,. . . or intrastate telemarketing." (H. Rep. at 3) Second, it specified that no section of the DNCA ". . . should be construed by the FTC to confer any additional authority to regulate common carriers . . . under the Federal Trade Commission Act." (H. Rep. at 9)

The FCC has acted promptly to meet its DNCA rulemaking obligation. On March 25, 2003, two weeks after the DNCA became law, the FCC issued a request for comments and reply comments to determine how the FCC could best fulfill its responsibilities under the DNCA. The comments and reply comments were filed last month, putting the FCC in a position to meet the DNCA's 180 days from enactment deadline for issuing revised and final rules.

This is simply the latest example of the FCC aggressively fulfilling its duty to ensure that carriers treat consumers fairly and honestly or be held accountable for their failure to do so. The FCC, at the direction of Congress, has already fully occupied the field when it comes to the practices of *interstate* carriers. With respect to *intrastate* carriers, the states continue to have full authority to regulate practices affecting consumers and competitors pursuant to existing state laws.

C. The FCC Has Pursued Enforcement Actions Against Telecommunications Carriers

When I testified before the Committee last year, I presented to you a chart that demonstrated that the FCC had in fact taken significant enforcement actions against unfair and deceptive practices with respect to telemarketing and the sending of faxes. The enforcement actions have continued at an accelerated pace as demonstrated by the list of enforcement actions and sanctions that follows this testimony and which comes directly from the FCC's website.

USTA believes that the FCC has demonstrated a commitment to enhancing its enforcement efforts, and it has held carriers and others within its jurisdiction accountable when they have violated laws or FCC regulations. There is, in USTA's judgment, no need to insert confusion or duplication by conferring jurisdiction over carriers to another independent regulatory agency, the FTC. If the FCC did not have the requisite authority to protect consumers, or if it failed to fully exercise its authority, there might be cause to accede to the request of the FTC for concurrent jurisdiction. This, though, is not the case. There is no regulatory failure that USTA has observed nor has USTA seen evidence of a gap between the FCC's and FTC's jurisdiction that requires rescission of the common carrier exemption to the FTC's jurisdiction.

D. Conclusion

The FCC comprehensively regulates unjust, unreasonable and deceptive consumer practices by carriers and their agents, and it is fully engaged in effectuating the competition provisions of the 1996 Act. To add concurrent FTC jurisdiction is unnecessary and would potentially produce conflicts with the comprehensive regulatory scheme found in the Communications Act and administered by the FCC.

Extending concurrent jurisdiction to the FTC over telecommunications common carriers would be counterproductive as it would lead to carrier and consumer confusion. Carriers would not know which agency to rely on for advice or which agency's compliance standards to follow. Consumers would have to discern the differences between FCC and FTC processes and standards. There being no compelling demonstration of a failure by the FCC to ensure that consumers are fully and fairly protected from unjust, unreasonable or deceptive carrier practices, USTA asks that you not grant the FTC concurrent jurisdiction with the FCC over carriers.

Thank you.

Marketing Enforcement Actions

Detailed Information

04–07–2003	*Hearing* ordered to determine whether to revoke the common carrier operating authority of affiliated long distance companies NOS Communications, Inc., Affinity Network Incorporated, and NOSVA Limited Partnership for apparently engaging in deceptive and misleading marketing practices
12–26–2002	*$1,000,000 Consent Decree* with NOS Communications, Inc. and Affinity Network Incorporated for unfair and deceptive marketing practices
04–02–2001	$1,000,000 in total fines proposed in Notice of Apparent Liability against *NOS Communications, Inc. (NOS) and Affinity Network Incorporated (ANI)* for apparent unfair and deceptive marketing practices
12–07–2000	Order On Reconsideration of 7/17/00 Order imposing a forfeiture against *Business Discount Plan, Inc.* (denied in part, granted in part). Forfeiture adjusted to $1,800,000
07–17–2000	$2,400,000 forfeiture assessed against *Business Discount Plan, Inc.* for slamming violations and telemarketing abuse
03–01–2000	FCC/FTC *Policy Statement* on Deceptive Advertising of Long Distance Telephone Services
03–01–2000	$100,000 Consent Decree with *MCI WORLDCOM* for marketing and advertising practices

Telephone Solicitation

Detailed Information

06–03–2003	*Citation* issued to Bill Currie Ford, Inc. (a.k.a. Bill Currie Pre Owned Centers), Tampa and Brandon, Florida for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
05–20–2003	*Citation* issued to Energy Windows Plus, Inc., a.k.a. FLA. Patio Rooms, Inc., Waterford, Michigan for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
05–13–2003	*Citation* issued to Far Star Enterprises (d/b/a/Nu-Cote Exteriors), San Diego and La Jolla, California for violation of the TCPA and Commission's rules regarding honoring do not call requests
04–29–2003	*Citation* issued to Warrior Custom Golf, Inc., Irvine, Fullerton, and Lake Forest, California for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
04–22–2003	*Citation* issued to 1 Home Lending Corporation, Calabasas, California for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines

Telephone Solicitation—Continued

Detailed Information

04–08–2003	*Citation* issued to Bridge Capital Corporation, Lake Forest and Mission Viejo, California for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
04–01–2003	*Citation* issued to Dura-Plex, Inc. for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
03–11–2003	*Citation* issued to Express Consolidation, Inc., Delray Beach, Florida for violations of the Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
02–25–2003	*Citation* issued to National Cleaning Service (d/b/a Albanez, Inc. and Jani-King), Rockville, Maryland for violations of the Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
02–19–2003	*Citation* issued to California Express Funding, Ontario, California for violations of the Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
02–12–2003	*Citation* issued to Spry Group, Hamilton, Ohio for violations of the Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
01–28–2003	*Citation* issued to Lifetime Capital Guarantee (dba/Rue Educational Publishers), Clearwater, Florida, and C.T. Corporation System, Indianapolis, Indiana for violations of the Commission's telephone solicitation rules, by delivering prerecorded messages to a cellular telephone line
01–14–2003	*Citation* issued to Michigan Soft Water of Central Michigan, Inc., East Lansing and Grand Rapids, Michigan for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines and honoring do not call requests
12–20–2002	*Citation* issued to Captain Clean Carpet Care, Newark, California; and, Maharam Fabric Corporation, Hauppauge and New York, New York for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
12–17–2002	*Citation* issued to Chon-Ji Academy of Martial Arts, Inc., Teaneck and Closter, New Jersey for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
12–10–2002	*Citation* issued to Newgen Results Corp., San Diego, California and Lawrenceville, Georgia; and, TeleTech Holdings, Inc., Englewood, Colorado for violations of the TCPA and Commission's rules regarding honoring do not call requests
12–03–2002	*Citation* issued to Inbound Calls, Inc. (dba/ICI, The Call Center, and Family Travel), Carlsbad and San Diego, California for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
11–26–2002	*Citation* issued to JZA Development Corporation (dba/University Painters, Inc.), Alexandria, Virginia, King of Prussia, Pennsylvania, and Chevy Chase, Maryland for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
11–12–2002	*Citation* issued to Executive Carpet & Beyond, Inc., Stamford, Connecticut for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
11–05–2002	*Citation* issued to American Life and Health Insurance, Arlington and Pasadena, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines

Telephone Solicitation—Continued

Detailed Information

10–29–2002	*Citation* issued to Silverleaf Resorts, Inc., Dallas, Texas; and, P & M Consulting, Inc., Grandview, Missouri and Overland Park, Kansas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
10–22–2002	*Citation* issued to Integrated Chiropractic Clinic (d/b/a Grenda Chiropractic and Grenda Family Chiropractic), Torrance and Redondo Beach, California for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
10–15–2002	*Citation* issued to A Friendly Carpet Cleaning, Lodi, New Jersey for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
10–08–2002	*Citation* issued to Accurate Collision Repair, Inc., Columbus, Ohio for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
08–06–2002	*Citation* issued to Michael Miller Insurance Agency (aka MMB Insurance, et.al.), Worthington and Columbus, Ohio for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
07–30–2002	*Citation* issued to Citywide Financial Group, Inc., Long Beach, California for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
07–23–2002	*Citation* issued to Centerpointe Real Estate, Inc., Norwalk, California for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
07–18–2002	*Citation* issued to Ad Resources, Inc. (dba/Dining and Shopping Spree and Conroe Dining and Shopping Spree), Houston, Temple, and Austin, Texas and Specialized Marketing Consultants, Houston, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines and honoring do not call requests
07–16–2002	*Citation* issued to Bolsa Financial, Inc. (dba/Bolsa Financial and Country Knoll Real Estate), Norwalk, California and Mr. Steven Harmon, Pasadena, California for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
07–09–2002	*Citation* issued to Argo Futures Group, Inc., Cleveland, Willoughby, and Chagrin Falls, Ohio and Ms. Sandra L. Allen, Willoughby, Ohio for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
06–25–2002	*Citation* issued to Network Traffic Controllers, Inc., Richardson, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
06–18–2002	*Citation* issued to Ameriquest Mortgage Company, Orange, California and Houston, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
06–11–2002	*Citation* issued to Wellness Chiropractic (dba/AAA Chiropractic, LaGrange Wellness Chiropractic and Carrollton Wellness Chiropractic), Louisville, La-Grange and Carrollton, Kentucky for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
06–04–2002	*Citation* issued to Insight Dynamics Corporation, San Ramon, California for violations of the TCPA and Commission's rules regarding unsolicited fax advertising
05–28–2002	*Citation* issued to Direct Data USA (dba/Auto Pro Finance, Dealer Information Service, and Beyond Your Expectations), Houston and Sugarland, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines

Telephone Solicitation—Continued

Detailed Information

05–07–2002	*Citation* issued to Funeral and Cemetery Finders Association, Pearland, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
04–30–2002	*Citation* issued to Legal Services Group Automotive, d/b/a LSG Auto Finance and LSG Auto Service, Missouri City, Stafford and Houston, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
04–16–2002	*Citation* issued to Vital Living Products, Inc., Matthews and Charlotte, NC for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
04–02–2002	*Citation* issued to Brentwood Capital Corporation, Brentwood, Tennessee for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
03–19–2002	*Citation* issued to White Rock Wildcats, Inc., Dallas, Texas for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
03–05–2002	*Citation* issued to American Marketing Associates, Inc., Annapolis and Brandywine, MD, and Vandergriff Chevrolet, Arlington, TX for violations of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
12–18–2001	*Citation* issued to Logistical Services, Inc d/b/a Stones Gym and Stones Family Fitness Center, Friendswood, TX for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines
12–18–2001	*Citation* issued to Sunset Home Improvements, Inc., El Segundo, CA for violation of the TCPA and Commission's rules regarding transmitting prerecorded unsolicited advertisements to residential telephone lines

Senator SMITH. Thank you.

Mr. Cooper, Mr. Schwartz, I do not want to be unfair to you. We can recess, and I can go vote and come back, or—let's take it, then.

STATEMENT OF SCOTT COOPER, MANAGER, TECHNOLOGY POLICY, HEWLETT-PACKARD COMPANY

Mr. COOPER. I will try to make three points, very briefly.

One, HP thinks that the FTC is not only a leader in consumer protection in this country; we also think it has been a great role model for what other consumer-protection agencies should do around the world. We think that it leads by example. And I think that the cross-border fraud provision is an example of that. We have some concerns, and we will get into it very briefly.

We think that the fact that the FTC is leading this effort to create a seamless network of enforcement on a worldwide basis is extremely important. And the fact that the FCC does this in partnership with business, with consumer groups, and that it has been a very forthcoming effort to make this ecumenical, I think, is an example of what works in the United States that we wish would work in other places around the world.

We certainly found, in other Nations, that they are doing reviews of their consumer-protection laws. They are finding, in many cases, that they are being too prescriptive, that they are too detailed, and they do not work in the real world. Unfortunately, we still find, in many places around the world, that consumer-protection agencies

do not see business, or even consumer groups, as potential partners in this effort toward creating a regulatory environment.

I think, in a lot of places in the world, that self-regulation is seen, unfortunately—and, unfortunately, in many cases, it has been proven true—as non-regulation. We do not think that is true in the United States, where we have, through groups like the Better Business Bureau, that handle 3 million consumer disputes a year, a very good model of self-regulatory dispute resolution that blends itself very nicely with the legal enforcement that the FTC does. And we think that that continuum that, when, say, the BBB discovers cases of potential fraud or patterns of abuse, they feel they have an obligation to pass that on to local law enforcement authorities with the FTC. We wish that kind of model would be used other places around the world.

The second point I would like to very quickly make is that just last month, a group of business leaders called the Global Business Dialogue in Electronic Commerce reached an agreement with Consumers International on guidelines for what dispute resolution should look like on a cross-border basis. Well, this is important, in itself, for offering consumers opportunities to resolve basic garden-variety disputes. Again, it is going to help legal authorities, because when dispute providers discover potential fraud on a global basis, they also will have the obligation, under these guidelines, to pass that on to local law enforcement authorities for them to handle.

So we think that there are a lot of things going on in this field where there can be potential partnerships between legal authorities on one side, and businesses and consumers on the other.

The last point I would like to make is on the legislation, itself, being considered. We agree wholeheartedly with the FTC. We think we need cross-border fraud legislation. Where have concerns is really in two areas. One is that where we think—and this has been referenced before—what is being enforced should, indeed, be illegal under the U.S. law. And the second point is, is that when a foreign law enforcement agency brings a case to the attention of the FTC, there should be a compelling legal basis for the request for information sharing.

So we think that this legislation needs to be worked on, but it is something that can be worked on. The devils are always in the details. But we think it is very important to get this legislation up and through the Congress, hopefully this year.

Thank you very much.

[The prepared statement of Mr. Cooper follows:]

Prepared Statement of Scott Cooper, Manager, Technology Policy, Hewlett-Packard Company

Senator Smith and Members of the Committee, I am pleased to be here this afternoon to discuss—and support—the re-authorization of the FTC, as well as to talk about issues of consumer protection before the FTC and this Committee. Hewlett-Packard has long been active with the FTC in partnering on issues of global consumer confidence; HP has served on two recent occasions as the business representative to the U.S. delegation on Consumer Protection to the Organization for Economic Cooperation and Development (OECD). HP also serves as the chair of the Consumer Policy working group of the International Chamber of Commerce (ICC), and the chair of the Consumer Confidence committee of the Global Business Dia-

logue for electronic commerce (GBDe), an organization of 70 of the largest global businesses engaged in e-commerce.

HP believes that the re-authorization of the FTC is important not only because of the key role that the FTC serves in our country's consumer protection infrastructure, but also for the leadership role that the FTC has played on global consumer protection issues as well. The growing importance for world economies of the global marketplace has been in a sense a "forcing mechanism" requiring both government and business to react to rapid change that make old ways of doing business—or regulating business—are no longer as effective.

Governments, businesses and consumers must all feel confident that their interests are being protected in order for the global marketplace to grow and flourish. And the opportunities are there; while developed economies have been growing at a recent rate of 1.5 to 2.5 percent a year, electronic commerce in those same countries is growing at a rate of 30 to 40 percent a year. If approached in a collaborative manner, the global marketplace can empower consumers, expand business opportunities and act as a powerful driver for 21st century economic growth, but consumers and legitimate businesses must be able to confidently find each other in the global marketplace.

The FTC's global leadership is exemplified by the coordinating role that the Agency has played in organizing legal efforts in developed countries to combat global fraud. As well, the FTC has led by example, by finding practicable, collaborative solutions to issues of consumer protection. And part of that collaboration has been to reach out to businesses and consumer groups to include them in the decision-making process.

We have seen in recent years a number of cases where other countries have reviewed their consumer protection laws and have concluded that they may be too detailed, too proscriptive to keep pace with the growth and challenges of the global marketplace. But unfortunately, as well, many global consumer agencies still keep business at arms-length rather than looking for opportunities to join forces in combating 'bad actors' in the marketplace.

This global leadership shown by the FTC is especially pertinent in the area of combating cross-border fraud. In part, through its work in the OECD, the FTC has created a clearinghouse for consumer protection agencies in developed countries to share information about suspected cases of cross-border fraud. This clearinghouse, "econsumer.gov" is a necessary first step in creating a global response to a global problem; joining together the legal resources in both countries where fraudulent businesses reside, and where consumer victims live.

However, a problem that needs to be addressed in fighting global consumer fraud is incenting consumers to report disputes where they may have been victimized. This problem takes on many faces. First, consumers may not be aware that they are victims of a fraud until so much time has passed that redress becomes difficult. Second, consumers may be discouraged, embarrassed and/or cynical about the ability of legal authorities to resolve their dispute. And finally, consumers may not be aware of whom to turn to when they are victims.

Businesses (as well as consumer organizations) have a vested interest to help legal authorities combat cross-border fraud. If the global marketplace is considered a risky venue to undertake transactions, then neither businesses nor consumers will benefit from opportunities to meet and transact business. A first step towards creating confidence in the global marketplace is to create best practices for merchants who will serve the global marketplace. A second step is to create guidelines for the resolution of those consumer disputes that do arise. I am pleased to say that consumer groups and businesses have been meeting regularly over the past two years to develop just such guidelines.

Last month, Consumers International, (representing over 160 consumer groups world-wide), and the Global Business Dialogue for Electronic Commerce (representing 70 of the largest global businesses engaged in electronic commerce), reached an agreement on guidelines for the resolution of disputes that arise between merchants and consumers in cross-border transactions. These 'rules of the road' also include specific recommendations for the development of third-party dispute settlement experts (called ADR for alternative dispute resolution), and recommendations to governments for facilitating the growth of global ADR settlement processes. This now-successful negotiation between consumer groups and business of creating ADR mechanisms has also had the strong support of the FTC, as well as the European Commission, METI in Japan and other government groups.

While the resolution of "normal" consumer disputes may seem a far cry from combating hard-core fraud, the development of a dispute resolution infrastructure can help in two important ways:

(1) Consumers need to be made aware as quickly as possible when they may be victims of fraud so that authorities can respond effectively. In the United States, the Better Business Bureau handles over 3 million consumer disputes a year. Some of these disputes turn out to be cases of fraud, but could not necessarily be identified as such until a pattern of abuse could be identified by the BBB. Thus ADR providers such as the BBB may hear of fraudulent scams before legal authorities are aware of them.

(2) When patterns of abuse are identified, dispute resolution providers must alert legal authorities. Legal authorities will only uncover a fraction of the cases of fraud that may occur. Adding dispute resolution providers as extra 'eyes and ears' to uncover potential fraud can be of great value to law enforcement.

Creating this continuum of enforcement—from simple consumer dispute resolution to uncovering patterns of abuse—will create a partnership of consumer groups, businesses and legal authorities in combating cross-border fraud. I am therefore pleased that in the FTC's draft legislation recognizes the usefulness of private entities that "voluntarily provides material to the Commission that it reasonably believes is relevant to a possible unfair or deceptive act or practice as defined in Section 5(a) of [the FTC] Act."

With the encouragement of the FTC, as well as commensurate legal authorities in Europe, Japan, China, Chile and elsewhere, a number of organizations such as the BBB are joining together to offer consumers dispute resolution services in the global marketplace. And part of their obligation to consumers will be to report suspected cases of fraud or deception to the proper legal authorities. Governments also need to encourage consumers to take advantage of ADR services; not only because resolving consumer disputes with benefit their citizens, but also because in doing so, cases of fraud can be quickly identified and brought to the attention of legal authorities.

We have also appreciated the opportunity to review the draft language provided by the FTC on cross-border fraud. Hewlett-Packard is very supportive of the goals of this legislation, and would be pleased to work with the FTC and the Committee in refining the actual language of the proposed legislation. In particular, we are concerned about the seeming wide range of enforcement that could be utilized by foreign agencies against U.S. citizens. There must be a high level of coordination between law enforcement in the U.S. and abroad if efforts to combat global fraud are to be successful, but this collaboration must be based upon two important concepts:

(1) That what is being enforced is indeed illegal under U.S. law; and

(2) That the foreign law enforcement agency must set forth a compelling legal basis for its request for information sharing.

Having said that, HP believes that this legislative proposal is an important step in creating a seamless level of consumer protections in the global marketplace. We look forward to working with the Committee in this effort.

ALTERNATIVE DISPUTE RESOLUTION GUIDELINES—MAY 2003

AGREEMENT REACHED BETWEEN CONSUMERS INTERNATIONAL AND THE GLOBAL BUSINESS DIALOGUE ON ELECTRONIC COMMERCE

Introduction

Electronic commerce, especially between consumers in one country buying goods or services from businesses based in other countries, will grow unabatedly only if consumers feel confident that their interests are sufficiently protected in the case of disputes. At the same time, there is also the concern that merchants—especially small and medium sized enterprises (SMEs)—might be faced with unmanageable problems due to difficulties related to consumer disputes resulting from Internet transactions.

Recourse to courts in disputes resulting from international Internet transactions is often complicated by the difficult questions of which law applies, and which authorities have jurisdiction over such disputes. Furthermore, international court proceedings can be expensive, often exceeding the value of the goods or services in dispute. If this were the only means to settle disputes, it would certainly not enhance consumer confidence in international electronic commerce and would strongly induce merchants to restrict the geographic scope of their offers. This, in turn, would limit competition and consumer choice.

There are widely differing views held among governments on the right type and level of consumer protection, even at the regional level of the European Union or the U.S. Complete international harmonization of applicable laws and international

agreements on competent jurisdictions might be the ideal solution in theory, but it is unlikely that this can be achieved satisfactorily in practice in the near future.

The situation is at least as difficult with regard to the issue of the competent forum. Business acknowledges that the application of the "country of origin" principle alone may not be sufficient to boost trust in online transactions, since consumers are unlikely to resort to the courts of other countries where merchants are resident. Conversely, the application of the "country of destination" principle (the residence country of the customer) is not the right answer either, since merchants will be unenthusiastic about international transactions that could subject them to a variety of differing country laws, processes and legal reach of every country in which their online customers may live. Moreover, for consumers this principle may only provide illusory protection, as in many cases the cost and complexity of cross-border enforcement stands in the way of effective redress.

Probably the best way out of this dilemma and an important catalyst for consumer confidence in electronic commerce is that Internet merchants offer their customers attractive extra-judicial procedures for settling disputes as an alternative to the cumbersome and expensive resort to courts.

In the offline world such alternative dispute resolution (ADR) systems are being used quite successfully as an effective, quick and efficient method for addressing consumer complaints that are not resolved through a simple contact with the company (in the framework of customer satisfaction systems) and there is already—at least in some parts of this world—some limited but positive experience with ADR related to business-to-consumer Internet transactions.

Through ADR, consumers' concerns can be addressed fairly and in a timely manner. ADR allows both parties to avoid the delays and the costs of appealing to either a government administrative agency or the courts. In addition, the use of ADR avoids overburdening both administrative and judicial systems (even when small claims courts exist), while at the same time, in general, preserving the consumers' right to seek legal redress should they be dissatisfied with the results of the ADR process. Finally, ADR can be more flexible and creative in finding solutions that satisfy both parties, while consumer protection agencies and/or courts may offer only limited remedies in resolving disputes, particularly where those remedies are prescribed by law or regulations.

This GBDe paper has been written based on the practical experience of a vast number of companies and business associations, including private sector organizations offering online ADR systems, from all parts of the globe. Its content has been discussed and developed with contributions from governments and representatives of consumer organizations as well.

This paper makes recommendations to Internet merchants, ADR service providers and governments. Guidance is given for the use and development of ADR systems, and recommendations are put forward for government policy actions geared at meeting the requirements of business for effective ADR and creating high levels of consumer confidence in e-commerce.

Definitions

The term "Alternative Dispute Resolution (ADR)" in these recommendations covers all methods of resolving disputes related to obligations resulting from contracts concluded "electronically" (primarily over the Internet) between professional sellers of goods or providers of services and final consumers (B2C), operated by impartial bodies other than courts of law.

More specific distinctions within the ADR concept, such as "arbitration", "mediation" and "conciliation/negotiation", are often used interchangeably and without much precision. Such distinctions may, however, be of relevance with regard to the role of the dispute settlement officer(s) in the process and the enforceability of the results.

"Arbitration" usually is a process whereby one or several independent arbiters invite the parties to submit the facts and their arguments (oral and/or written procedure) and finally decide on the basis of equity or law. Arbitration, by definition, is normally final and binding, and thus may not—in most cases—lend itself easily to the non-jurisdictional world of trans-border business-to-consumer transactions.

"Mediation" normally is a process whereby a mediator simply passes the proposal of settlement to the other party and the counterproposal back to the first party until the two have reached agreement. The mediator does not intervene in the negotiations but registers only the final agreement. When agreed to by both parties, the successful results of mediation are legally a contract and are enforceable in this capacity.

"Conciliation/negotiation" normally is a process whereby an independent conciliator actively guides the parties towards a fair compromise. This process does not

develop in a legal vacuum, but need not investigate in detail the applicable law. The parties' understanding of the legal rights and obligations (which may be conflicting) certainly plays a role, but equity might be the deciding factor. If the (final) conciliation proposal meets the agreement of both parties it becomes a contract and is enforceable in this capacity. If the parties do not agree on any compromise, they are free to go to court.

Purely internal dispute settlement services that are offered by merchants as an after-sale service rooted in good commercial sense, rather than as an alternative to court procedures, may not provide sufficient guarantees of impartiality to assure consumers that they will be able to obtain redress in the event of a disagreement over a transaction. Of course, wherever possible, direct business/consumer resolution is and will be the preferred instruments for solving customer complaints in B2C Internet transactions. These services are referred to here as "customer satisfaction systems," and they may become a step in the chain of redress, *e.g.,* if customers wish to make use of ADR offered by the merchant, they may be invited to submit their complaint first to such a service (call centers, complaint services, etc.) before filing it with the ADR officer.

Scope

These recommendations deal exclusively with business-to-consumer (B2C) disputes in electronic commerce, where ADR is still relatively little known and practiced. Settlements of disputes resulting from business-to-business (B2B) transactions, both offline and online, will follow their own rules with a very high degree of party autonomy, mostly in the form of binding arbitration. The issues of consumer protection and consumer confidence are of no relevance in this context. Hence, there is neither a need to develop new recommendations for B2B ADR, nor would it be appropriate to address any issues related to B2B under the same parameters as B2C dispute settlements.

A survey of ADR systems for B2C Internet transactions already functioning or in the process of being established shows that most of them are established upon the initiative of groups of business companies (including auditing firms, banks, insurance companies, law firms), business associations, institutes (including universities), or consumer organizations, often as independent businesses. They cover their costs by sponsor and user fees, sponsors being normally those merchants that offer the services of this specific ADR system to their customers. In some instances they are also offered government funds, notably to function as pilot projects. Although only theoretical today, one should not preclude ADR systems being established by individual merchants, if a sufficient degree of impartiality is guaranteed.

The recommendations to business contained in this paper are addressed both to Internet merchants who signal to their customers that they recommend submitting disputes to ADR, and to organizations that provide ADR as a service.

Recommendations to Internet Merchants

Encourage the use of in-house customer satisfaction programs

As a first and preferred remedy in any dispute, Internet customers should be offered access to in-house customer satisfaction systems. Depending on the type of transaction and the nature of the system, such approaches may serve as a valid alternative to ADR. For example, a merchant involved in the sale of low-priced merchandise might choose to offer an unconditional money-back guarantee to all customers rather than establishing an ADR system. In any event, it appears advisable to request that customers direct any complaint first to an in-house customer satisfaction system prior to taking advantage of any ADR mechanism.

Propose the possibility of ADR

Unless full customer satisfaction is guaranteed by in-house systems, customers of merchant websites used for B2C transactions should be notified that the merchant is ready to submit disputes resulting from online transactions to one or more specified ADR systems. Information about dispute resolution via ADR should be provided as a part of the overall information, perhaps in the framework of a reference to a code of conduct (Trustmark) or as a part of the general sales conditions.

ADR should be presented as a voluntary option for consumers if a dispute arises, not as a contractual obligation.

Binding Arbitration

Merchants should generally avoid using arbitration that is binding on consumers because it may impair consumer confidence in electronic commerce. Arbitration that is binding on merchants as an obligation of membership in a trustmark program, on the other hand, serves to promote consumer confidence in electronic commerce.

Arbitration that is binding on consumers should only be used in limited circumstances, and where it clearly meets the criteria of impartiality, transparency and public accountability. Consumer decisions to engage in binding arbitration must be fully informed, voluntary, and made only after the dispute has arisen.

Inform about conditions of ADR

Potential customers should be informed about the conditions of access (online or other), the cost (free of charge, nominal fee, cost borne by the merchant, etc.), the legal nature of the ADR (arbitration, mediation, conciliation, negotiation, etc.) and of its outcome (binding/not binding/binding for the merchant; enforceable), and recourse to other instances, notably to law courts.

No Retaliation

Merchants should not take any retaliatory action against customers because they have initiated contact with an ADR service concerning a dispute.

Recommendations to ADR Service Providers

Impartiality

The ADR personnel must be impartial, in order to guarantee that decisions are recognized as being made independently, thus strengthening the reputation and credibility of the organization providing ADR. Impartiality must be guaranteed by adequate arrangements, which may include measures such as the establishment of appropriately composed supervisory bodies or the appointment of dispute resolution officers according to specific criteria. The governing structure of the ADR service should be designed so as to ensure neutrality in all respects.

Dispute resolution personnel must be insulated from pressure to favor merchants or consumers in resolving disputes. When the amount in dispute is important and/or when ADR is finally binding for both parties, even higher standards of transparency should be respected, including *e.g.,* that the names of dispute resolution officers are made known to the parties, who should have the right to challenge them for cause. When a merchant uses a particular arbitration service repeatedly, to the extent practicable, the ADR officers who handle the disputes should be rotated to ensure their continued impartiality.

Qualification of ADR officers

Dispute resolution officers should have sufficient skills and training to fulfill the function in a satisfactory manner. Formal lawyer qualification and license should not be required.

Accessibility and Convenience

ADR systems must be easily accessible from each possible country. Online access might be the preferred choice. Requirements about the form of the submission of a case should be kept to the necessary minimum. Customers should receive maximum guidance in filling in and filing submissions. Appropriate solutions must also be found for any problems that may result from different languages used by the merchant, the ADR service provider and the customer.

Speed

To be effective, ADR systems must resolve disputes quickly if they are to meet the needs of both consumers and businesses. In any case, they must be speedier than courts in providing satisfactory results.

Low cost for the consumer

The ADR service should be provided to the consumer at no or only moderate cost, while taking into account the need to avoid frivolous claims. An impartial screening process provided by the ADR system could do this. Prior submission of a complaint to a customer satisfaction program will also permit an early assessment of the real nature of the claim.

In fact, the cost of ADR will be significantly lower for both consumers and businesses than formal administrative or legal actions. This is particularly true when costs are calculated in terms of both time and money and where formal actions involve time-consuming depositions, hearings, legal representation, and personal appearances requiring international travel.

Transparency

ADR systems should function according to published rules of procedure that describe unambiguously all relevant elements necessary to enable customers seeking redress to take fully informed decisions on whether they wish to use the ADR offered or address themselves to a court of law.

To ensure credibility and acceptance of an ADR system, information should include:

- the types of dispute which may be referred to the body concerned, as well as any existing restrictions in regard to territorial coverage and the value of the dispute;
- the rules governing the referral of the matter to the body, including any preliminary requirements that the consumer may have to meet (*e.g.,* to attempt first to get redress through a customer satisfaction system offered by the merchant), as well as other procedural rules, notably those concerning the written or oral nature of the procedure, whether it is conducted exclusively or partly online, whether oral hearings are possible or required (separate of either party or jointly), attendance in person or possibilities of representation, and the languages of the procedure;
- the decision-making arrangements within the body and its governing structure public listing of its personnel, the selection process of dispute resolution officers for individual cases and the possibilities of challenging them by the parties;
- the possible cost of the procedure for the parties, including rules on the award of costs at the end of the procedure;
- the type of rules serving as the basis for the body's decisions (legal provisions, considerations of equity, codes of conduct, etc.);
- the manner of proceeding, whether decisions are made public, confidentiality of the handling of submissions and of proceedings;
- enforceability of agreed upon resolutions and any other possibilities of recourse.

The ADR provider should publish an annual report enabling a meaningful evaluation of all ADR cases and results, while respecting the confidential nature of specific case information and data. Such evaluation should include—at a minimum—an aggregated list of cases received, cases settled prior to ADR resolution, cases settled by ADR resolution and cases not resolved. To the degree possible, such report should include information on whether cases settled prior to, and at settlement, were to the advantage of the consumer or the merchant. In cases where arbitration is binding on one or both of the parties, information should be available to the public about the identity of the merchant, the type of dispute, and to the degree possible, whether the dispute was resolved in favor of the merchant or the consumer.

Principle of representation

The ADR procedure should not deprive the parties of the right to be represented or assisted by a third party at all stages of the procedure.

Applicable Rules

One of the principal reasons why business, consumers and governments consider the development of ADR systems to be of such strategic importance for the enhancement of consumer trust in electronic commerce is that such systems can settle disputes in an adequate fashion without necessarily engaging in cumbersome, costly, and difficult research on the detailed legal rules that would have to be applied in an official court procedure. Governments in particular, must be confident that the rights of both consumers and businesses are protected, while at the same time avoiding actions that could adversely impact the growth of global electronic commerce.

ADR dispute resolution officers may decide in equity and/or on the basis of codes of conduct. This flexibility as regards the grounds for ADR decisions provides an opportunity for the development of high standards of consumer protection worldwide.

Consumer Awareness

Except in special cases where both consumers and merchants find special circumstances to agree to arbitration (see below), consumers will not alienate their right to go to court by electing to use an ADR mechanism.

ADR should be presented as a voluntary option for consumers if a dispute arises, not as a contractual obligation. Thus, an arbitration decision taken by the dispute resolution officer(s) may be binding on the parties only if they were informed of its binding nature in advance and accepted this. Equally, the merchant shall not seek a commitment from the consumer to use binding arbitration prior to the materialization of the dispute, where such commitment would have the effect of depriving the consumer of the right to bring an action before the courts.

Referrals to law enforcement

ADR service providers should refer disputes to the relevant law enforcement authorities, with the consumer's permission, when they have reason to believe that

there may be fraud, deceit or patterns of abuse on the part of the Internet merchant. In such cases, the merchant should be informed that such an action has been taken.

Recommendations to Governments

Studies on the legal frameworks for ADR have demonstrated that they are fragmented between international conventions and legal instruments at several levels (federal/state, community/national, etc.). As a consequence, ADR systems conceived for worldwide application must respect a number of—not always compatible—conditions. Several of these elements can be easily accommodated, like the requirement that a valid agreement to submit a dispute to ADR would have to be entered into only after the dispute has arisen. Other elements are more problematic to accommodate, *e.g.,* that certain national laws on encryption or authentication inhibit the proper level of confidentiality and security in online proceedings, or that some national laws do not permit the conclusion of contracts online.

On the other hand, many governments are on record that they share the GBDe position that ADR is an essential element for the proper functioning of e-commerce and for the enhancement of consumer confidence in this medium. Hence, the GBDe expects governments to adopt policy stances in line with this goal.

International rules on competent forum and applicable law

Although ADR can provide appropriate solutions for many disputes, it must be recognized that even in the most ideal of worlds a certain number of disputes will still end up in court. Therefore, and also because these questions may still be posed in some ADR systems, the GBDe wishes to state clearly that questions of jurisdiction and applicable law in electronic commerce still need to be dealt with urgently and in a manner that encourages both business investment and consumer trust in electronic commerce. The GBDe position on this was expressed in the "Paris Recommendations" of the "Jurisdiction" Working Group in 1999.

Encourage the use of customer satisfaction systems and of ADR

Actively promote public awareness of ADR systems and their role in resolving business-to-consumer commercial disputes. Acknowledge the continuous efforts by companies to set up customer satisfaction systems, which should be used first before starting either ADR or court proceedings against a merchant. Likewise, policies should encourage consumers to use available ADR systems instead of or before seeking recourse to courts.

Education and Training

Support and promote educational activities of ADR officers by ADR system providers.

Encourage effective ADR systems

It is our recommendation that governments encourage customer satisfaction systems as a first step in the chain of redress prior to resorting to ADR's. Governments should promote and facilitate the development of high quality ADR services that are independent, transparent cost-effective, flexible and accountable to the public, without discriminating among impartial services solely on the basis of who offers them. Achieving a sustainable level of competition among ADR providers and achieving reciprocal agreements among these should be a priority.

As with any decision to introduce regulation, the decision as to whether and how to adopt government accreditation proposals should only be pursued after careful consideration and balancing of interests. The development of accreditation systems must take into account the interests of consumers and businesses for fair, transparent and cost-effective processes and the overall objective of the successful development of electronic commerce.

Any government-backed assessment rules should be developed with input from consumer groups, businesses and other stakeholders. To the extent possible this should be coordinated with similar efforts in other countries and regions to ensure a high degree of harmonization between assessment efforts to promote the development of international principles and rules including self-regulatory codes. Independent assessment and ratings systems may also help promote consumer empowerment.

ADR on the basis of equity or codes of conduct

Allow ADR systems to function on the basis of equity, or codes of conduct. It should not be required that dispute resolution officers necessarily have formal lawyer qualification and license. In some countries, mediation/arbitration processes are

legally regulated to be conducted solely by licensed lawyers, but deregulation and an appropriate legal framework should be aimed for.

Global access to and application of ADR

Promote the development of globally applicable ADR systems, and take an international perspective on ADR by working with other governments and international organizations.

Application of modern technologies in ADR

Refrain from creating obstacles for the innovative use of technology to settle consumer disputes and eliminate obstacles, resulting primarily from legislation on authentication and security, to the application of an appropriate level of confidentiality and security in online ADR.

Procedural and form requirements for ADR should be kept to a minimum

Eliminate requirements in some legislation that ADR must follow nearly the same procedural requirements, as the court system. The same applies to certain form requirements that may impede the use of ADR in the online context. The parties to an ADR case should be free to structure the proceedings, as they desire, as long as there is full transparency and information about the consequences.

Adjust offline ADR requirements to the online context

Remove inhibitions in national legislation or international conventions to conclude contracts—including dispute resolution clauses—online and adjust existing legal and political frameworks for offline ADR to online requirements.

Policy cooperation between public and private sector

Ensure close cooperation between the public and private sector to maintain a balance in achieving a satisfactory variety of ADR systems, which reflect consumer and business needs and are easily understood by the customer.

Enforcement Actions

Take appropriate enforcement action when ADR services do not comply with their stated policies and procedures.

Senator SMITH. Thank you, Mr. Cooper. And thanks to Hewlett Packard for your presence in the State of Oregon. You are very welcome citizens there.

I am pleased to be joined by Senator Brownback, as a Member of this Committee, and I am going to go vote.

And so, Mr. Schwartz, he is going to get the gavel, and you take your time. I have a number of questions for several of you. I will submit them in writing and thank you, in advance, for your answers to those. And I appreciate very much the time each of you have taken to be a part of this very important hearing.

Mr. Schwartz? And then Senator Brownback.

STATEMENT OF ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. SCHWARTZ. Mr. Chairman, Senator Brownback, thank you very much, and thank you for coming and rescuing the Chairman——

[Laughter.]

Mr. SCHWARTZ.—so that I can go into a little bit more detail.

In my written testimony, I go into detail in several different areas, but I am going to focus specifically on privacy, in the interest of time here.

We have been impressed with the Commission's commitment of resources and intellectual capital on privacy. Most of the Commission's privacy work has been tied directly to its mission of preventing deceptive and fraudulent business practices. For example, in the area of spam, the Commission has focused action in the area

of fraudulent e-mail scams. In their privacy sweeps, they have conducted detailed reviews of privacy notices. This has allowed them to convince companies to post online privacy notices while helping to prevent vague and even fraudulent practices.

While this work has been successful, the work of the Commission in privacy areas, enabled by specific statute, demonstrates that the FTC already has sufficient expertise to take on more general privacy-protection responsibilities. The Commission has demonstrated a thoughtful and patient, yet innovative and ultimately workable approach to addressing privacy issues that has transcended the Administrations. An example of this is the Commission's work on the Children's Online Privacy Protection Act, also the slow but steady improvement of the complex area of financial privacy education and enforcement.

In each of these cases, the Commission has brought a wide range of players to the table to work out difficult issues during an iterative and inclusive process, and then taken action where the law has clearly been violated.

The Commission's work on the Do Not Call Telemarketing Registry also shows this comprehensive approach to developing sound privacy protection. The Commission has made it clear that it has no intention to ban telemarketing; but, instead, to give consumers more control over how and why calls come to their house at dinnertime. CDT looks forward to helping promote the registry when it goes in to effect next month.

To give the Commission broader authority in other consumer privacy-related areas, Congress must now pass privacy legislation. The full Commerce Committee has already taken this step by voting in favor of the Online Privacy Protection Act and the Spam Bill last year. We hope that you will move these issues forward again this year, and that the rest of Congress will follow your lead on this critical issue for the future of a network economy.

Thank you, again, for this opportunity.

[The prepared statement of Mr. Schwartz follows:]

PREPARED STATEMENT OF ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

I. Summary

Chairman Smith and Members of the Subcommittee, the Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about the Federal Trade Commission (FTC) and its role in consumer and privacy protection. We thank the Chairman for the opportunity to participate in this hearing and look forward to working with the Committee to develop policies supporting civil liberties and a vibrant communications infrastructure.

Over the past eight years the FTC's activities in the area of information privacy have expanded. The Commission has convened multiple workshops to explore privacy, issued several reports, conducted surveys, and brought several important enforcement actions in the area of privacy. The Commission's work has played an important role in bringing greater attention to privacy issues and pushing for the adoption of better practices in the marketplace.

Three years ago, CDT testified that "(t)he work of the Federal Trade Commission—through its public workshops, hearings . . . provides a model of how to vet issues and move toward consensus."

Chairman Muris has successfully continued the consultation and education process, working with public interest groups and industry on key issues and taking enforcement actions or instituting rulemakings on several important new fronts.

CDT and other public interest and consumer groups have been pleased with the Commission's thoughtful approach to creating a National "Do Not Call Registry."

The registry will provide consumers with an easy way to cut down on unwanted telephone calls and will offer industry a streamlined means of complying with the growing number of state and self-regulatory "Do Not Call" lists.

CDT has also been pleased with the Commission's extensive educational efforts with the public and industry on spam, privacy technologies, privacy notices, ID theft, wireless privacy, and other issues. It should be noted that each of these areas is clearly within the FTC's jurisdiction to prevent deceptive trade practices.

However, CDT would like to see the Commission use its resources to address unfair information practices as well as deceptive ones. These unfair practices include: lack of meaningful notice and choice; the ability to correct and amend personal information; and inadequate security safeguards.

It has long been CDT's belief that unfair information practices are already covered by the Commission's current authority. Yet, the long-standing hesitancy of the Commission to proceed has made it necessary for Congress to confirm this authority in law. Although Chairman Muris has suggested that general Federal privacy legislation is unnecessary, CDT sees an *urgent* need for legislation similar to the Online Privacy Protection Act that was passed by the full Senate Commerce Committee last year. Privacy protections in law—enforced by the FTC—are an essential ingredient of building and maintaining consumer confidence in the networked economy. We thank you, Chairman Smith, as well as Senator Hollings and the other Senators who worked so hard to move the issue forward in the Committee last year. CDT looks forward to continuing to work with you to see such a measure passed again this Congress and signed into law.

II. About CDT

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

III. The Role of the FTC as the Federal Government's Leader on Consumer Privacy Issues

The FTC has used its current jurisdiction to take basic steps to protect the privacy of Americans in several innovative and balanced ways. The Commission is the government's leader in consumer privacy policy and should be commended for its current work in the area given its limited view of its own jurisdiction.

In October 2001, Chairman Muris said that the Commission would increase privacy enforcement by 50 percent. According to internal figures, the Commission says it is on track to reach this goal. This dramatic increase was on top of the new attention given to privacy issues.

In particular, over the past two years, the Commission has worked in ten areas of interest to CDT:

1. Unsolicited Commercial E-mail (Spam)

This year, the Commission held a three day-long workshop on spam that addressed many of the key issues and focused attention on possible solutions to a problem that has become a plague on Internet communications. The Commission taken several useful steps:

- The Commission has created an educational Website for consumers and businesses. The site provides consumers with helpful information on how spam works, why they get spam, and how to decrease the amount of spam they receive. The site advises businesses on how to comply with a user's unsubscribe request.
- The FTC has also conducted several studies to test whether "unsubscribe" or "remove me" requests were being honored. The study reported that the majority of consumer requests were not getting through. The Commission thereupon sent out warning letters to spammers. These studies also helped to inspire a wider range of research on this understudied issue, including CDT's well-received report "Why am I Getting All of this Spam?" [1]
- The FTC has taken action against several spammers who allegedly sent out deceptive, unsolicited commercial e-mails and participated in Web fraud, including a 2002 case where the FTC joined several state law enforcement officials in the United States as well as four Canadian law enforcement agencies in bringing 63 different actions against various Web schemes and scams that targeted victims through spam.

[1] *http://www.cdt.org/speech/spam/030319spamreport.shtml.*

While the Commission, given its limited view of its jurisdiction, has taken these exemplary first steps in research, education and enforcement regarding unsolicited commercial e-mail, CDT would like to see it given more power to tackle fraudulent spam Further appropriate steps could be taken under some of the provisions in the CAN SPAM Act (S. 877), sponsored by Senators Burns and Wyden. CDT is hopeful that we can begin to turn the tide on spam while still protecting the First Amendment right of anonymous non-commercial/political speech online.[2]

2. Telemarketing Sales Rule—"Do Not Call" Registry

Under the 1994 Telemarketing and Consumer Fraud and Abuse Prevention Act,[3] the Commission was given the authority to regulate telemarketing sales. The Commission's regulations, named the Telecommunications Sales Rules (TSR), were put into effect in 1995.[4] The TSR placed some basic time, place and manner restrictions on calls and left the door open to revisiting the rule if it was not adequately protecting consumers.

Some have said that telemarketing is merely an annoyance and not a privacy concern and therefore stronger rules are not necessary. CDT disagrees. We define privacy as individual control over one's personal information. Control over one's telephone number and other personal information is central to privacy in the modern world.

The American public seems to agree with us. An AARP study of New Jersey residents showed that 77 percent viewed telemarketing first and foremost as an invasion of privacy; 10 percent a consumer rip-off, and only 2 percent a consumer opportunity.[5]

The Commission responded to the public concern about telemarketing with the creation of a "do not call" registry, similar to those already in existence in 15 states. On this proposal, by the way over 50,000 public comments were submitted to the Commission.[6] Over 90 percent of them support the registry.

CDT believes the "do not call" list offers the best, balanced solution for unwanted telemarketing. Telemarketing in banned, but consumers can decide what kind of marketing calls they want and when they want to receive them.

In our comments supporting the FTC's "Do-Not-Call" initiative we stressed that the list should not dilute or undercut the protections afforded consumers by the states against invasive telemarketing. Further, as we pointed out, it is critical that consumers are not charged a fee to be placed on the "Do-Not-Call" list—consumers' ability to protect the privacy of their personal information should not be contingent upon their ability to pay a fee.

CDT has been pleased with how the public process on this important issue has progressed. It has been a model example of how a complex but important issue can be addressed through an open, public process.

The fact that the "Do-Not-Call" list will open in two weeks is a testament to the Commission's commitment to this issue. We hope that the Committee will continue to help monitor the roll out of the list in its oversight role.

3. Privacy Education

The FTC has generally played a valuable role working with and educating the business community about privacy best practices and implementation of fair information practices.

This year the Commission has held two workshops on privacy technologies—one aimed at consumer technologies and one at businesses. CDT participated in both and used the first as a forum to introduce a set of Authentication Privacy Principles developed in cooperation with a large working group of companies and consumer groups.[7]

FTC Forums such as these are important tool in highlighting specific privacy issues and encouraging efforts to address them. CDT is encouraged by discussions with the Commission, which indicate that these workshops will continue to tackle issues arising in the marketplace, including the difficult issue of the future of identity management in the networked economy.

---

[2] For more information on CDT's views on the CAN SPAM act, please see our recent Policy Post *http://www.cdt.org/publications/pp__8.12.shtml*.
[3] 15 U.S.C. 6101–6108.
[4] 16 CFR Part 310.
[5] *http://research.aarp.org/consume/nj__telemarketing.pdf*.
[6] CDT's comments, filed in coalition of other consumer groups, can be found at: *http://www.ftc.gov/os/comments/dncpapercomments/04/consumerprivacyguide.pdf*.
[7] The Interim Report of the Authentication Privacy Principles Working Group can be found at: *http://www.cdt.org/privacy/authentication/030513interim.pdf*.

4. Identity Theft and Identity Fraud

The FTC has been a leading agency in the prevention and prosecution of identity theft through. The Commission's identity theft program contains three key elements: the Identity Theft Data Clearinghouse;[8] consumer education and assistance resources; and collaborative enforcement efforts involving criminal law officers and private industry.

The most recent reports indicate that the Identity Theft Clearinghouse holds more than 170,000 victim complaints and serves as an important tool for 46 Federal and 306 state and local law enforcement agencies, including the U.S. Secret Service, the Department of Justice, the U.S. Postal Inspection Service, and the International Association of Chiefs of Police. The FTC has also been increasing outreach programs to educate law enforcement officials on how the Clearinghouse database can be used to enhance investigations and prosecutions.

In regards to consumer education and assistance resources, the FTC has held training seminars for law enforcement officials at all levels in an attempt to give law enforcement the necessary tools they will need to combat identity theft. The FTC has also implemented a nationwide, toll-free hotline that consumers can call if they have become a victim and a Website that consumers can access to file a complaint and gain helpful prevention tips.

The Commission's efforts in this area show that it can be a leader with other law enforcement agencies, serving as the main contact to the public. We hope that the Commission's work can help to cut down on what many believe to be the fastest growing crime in the country.

5. COPPA Compliance

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA)[9] in order to protect children's personal information in interactions with commercial sites. The FTC was required to enact a rule to implement COPPA and in doing so it clarified issues concerning coverage and liability, modified several definitions that would have interfered with children's ability to participate, speak and request information online, and made every effort to create a predictable and understandable environment for the protection of children's privacy online.

Since issuing its final Rule implementing COPPA, the FTC has taken several effective and necessary steps to enforce and enhance compliance with COPPA. In February 2003, the FTC took its most aggressive action yet to ensure children's privacy online by filing separate settlements with Mrs. Field's Cookies and Hershey Food Corporation for violating the law.

While there is still work to be done, we believe that COPPA has been successful in improving protection of children's privacy online. This experience demonstrates that the FTC can develop workable privacy rules in complex and sensitive areas that go well beyond its traditional arenas.

6. Gramm-Leach-Bliley Compliance

It is generally recognized that, across the financial service industry, the privacy provisions of GLB have proven unsatisfactory in scope and implementation—specifically on the issue of notice. A range of institutions have provided consumer notice that is so detailed and legalistic as to be largely worthless. If nothing else, the experience offers a lesson to policymakers seeking to impose and enforce privacy notice requirements.

Under GLB, the Commission has jurisdiction over important financial institutions such as insurance and mortgage companies. In an August 2001 survey, CDT found that these companies were among the worst in posting privacy notices on Websites. That month, we filed a complaint with the FTC about several mortgage companies that were not posting notices as required by the FTC's GLB regulations. While the Commission has not officially closed the case, the five remaining Websites have now posted privacy policies.

CDT believes that there is more basic, but important enforcement work that the Commission could to do in the area of privacy notices for insurance and mortgage companies. Especially, the Commission could play a leadership role in moving the companies under its GLB jurisdiction toward simple clear and more meaningful notices.

7. Computer Security Education

The FTC has taken several steps to educate consumers on computer security. In addition to holding workshops, the FTC has created a helpful guide for consumers

[8] *http://www.consumer.gov/idtheft/.*
[9] 15 U.S.C. 6501.

on how to stay safe online using a high-speed Internet connection. The guide details how users can protect their computers from viruses and hackers by explaining security features such as firewalls and updating virus protection software. The FTC has worked diligently to make the report both understandable and appealing to the average consumer through careful analysis and easy to read text. Led by Commissioner Orson Swindle, the Commission has continued to work with consumer groups to ensure that the guide is easy to use and contains the necessary information.

8. Internet Privacy Sweeps

Last year, the Commission continued its ongoing assessment of the state of Internet privacy which began five years ago and has been repeated twice since. The Commission embraced a report [10] organized by the Progress and Freedom Foundation and conducted by the Ernst and Young accounting firm. The results show significant improvement in the number of privacy policies posted and the growth of the new privacy protocol, the Platform for Privacy Preferences (P3P).[11] This positive growth is due, in part, to the educational work of the Commission.

On the other hand, the study found that self-regulatory seal programs have actually been shrinking. This is mainly due to the bankruptcy of many dot com players, but it also indicates that we are entering a time of a major privacy gap. Some companies are actively involved in the privacy issue and are doing their best to build trust . Meanwhile, a small number of free-rider companies are doing no work on privacy. The marketplace has remained confusing to the average consumer and many prefer to sit on the sidelines until baseline privacy is assured.[12]

CDT hopes that Congress will continue to support and monitor the FTC's privacy sweeps—and we urge the Commission to work with a wide range of organizations and academics, including consumer groups, when preparing the parameters and methodology for future sweeps.

9. Wireless Privacy

In December 2000, the Commission held a workshop entitled "The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues." [13] As this subcommittee knows well, the wireless privacy issues have been a growing concern for consumers due to the emerging use of location tracking technologies to provide consumers with enhanced services. It was clear from the workshop that the staff and Commissioners have the understanding and skills necessary to undertake a serious investigation of privacy and security in this area. However, the Commission has taken little action in this area since the workshop. CDT urges the Commission to follow-up with another workshop in this area as wireless technologies and location applications progress.

10. Online Profiling and Data Mining

Online profiling is the practice of aggregating information about consumers' preferences and interests, gathered primarily by tracking their movements online. It remains one of the most complex and opaque issues in privacy. Consumers are concerned because they know someone is watching, but they don't know who, how or to what end.

In November 1999, FTC examined online profiling, focusing on the use of the resulting profiles to create targeted advertising on Websites.[14] In July 2000, the FTC issued a two-part report on online profiling and industry self-regulation.[15] The Commissioners unanimously commended the Network Advertising Initiative (NAI) for its self-regulatory proposal that seeks to implement Fair Information Practices for the major Internet advertisers' collection of online consumer data. The July report also asked Congress to enact baseline legislation to protect consumer privacy. In addition

---

[10] *http://www.pff.org/pr/pr032702privacyonline.htm*.

[11] CDT was the originator of the P3P concept and has continued to work on the specification and its adoption. More information about P3P can be found at *http://www.w3.org/p3p and http://www.p3ptoolbox.org*.

[12] *Business Week* has conducted a number of surveys showing that privacy is the number one concern of both those who are not online and those who are online, but do not shop online. The most recent is available at *http://businessweek.com/2000/00__12/b3673006.htm*. Jupiter Communications has estimated that $18 billion in consumer transactions did not take place online because of privacy concerns (McCarthy, John, "The Internet's Privacy Migrane," presentation, SafeNet2000, December 18, 2000].

[13] A staff summary of the event was released in February 2002 *http://www.ftc.gov/bcp/workshops/wireless/*.

[14] Public Workshop on "On-Line Profiling"—*http://www.ftc.gov/bcp/profiling/index.htm*.

[15] *http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf* and *http://www.ftc.gov/os/2000/07/index.htm#27*.

to its several reports, the FTC has also held a series of public workshops on data mining in an effort to educate consumers as well as it itself.[16]

Especially important are the issues of government mining of commercial databases in the name of national security or other objectives. FTC examination of data quality issues could serve to be extremely useful.

The reports and workshops that the FTC has undertaken in this area have represented the best work done in this area internationally. Unfortunately, since Chairman Muris has taken office, little public work has been continued in this area. We hope that the Commission will return to this area, one that causes concern to so many consumers.

III. The Future Role of the FTC in Privacy Issues

While the Commission's privacy work has been successful, it has also been limited mainly to areas of deceptive or fraudulent practices. CDT believes that this limited focus is preventing the Commission from taking on urgently needed actions in the privacy area.

Proposed Privacy Legislation

CDT believes that a comprehensive, effective solution to the privacy challenges posed by the information revolution must be built on three components: best practices propagated through self-regulatory mechanisms including nonprofit,[17] commercial and governmental education efforts; privacy as a design feature in products and services; and some form of Federal legislation that incorporates Fair Information Practices—long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."[18] Legislation need not impose a one-size-fits-all solution. For broader consumer privacy, there need to be baseline standards and fair information practices to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies. Finally, there is no way other than legislation to raise the standards for government access to citizens' personal information increasingly stored across the Internet, ensuring that the 4th Amendment continues to protect Americans in the digital age.

On May 17, 2002 the Senate Commerce Committee passed the Online Privacy Protection Act. This important legislation would have set a true baseline of privacy protection and would give the FTC the clear authority to go after companies engaging in unfair information practices.

During the Committee process, Senator McCain asked the FTC Commissioners to give their views on the Online Privacy Protection Act. In response, Chairman Muris gave five reasons that such a bill was not necessary at that time.[19] CDT disagrees respectfully but strongly with the Chairman. While CDT continues to work with the FTC to help advance self-regulatory efforts, privacy enhancing technologies and public education, we believe that these efforts alone are not and cannot be enough to protect privacy or instill consumer confidence on their own.

CDT commends the Senate Commerce Committee for its excellent work on privacy issues. We hope that this Committee continues to push for the FTC's expanded jurisdiction in this area.

Proposed Rescinding of Common Carrier Exemption

The Committee also asked CDT to address the issue of rescinding the exemption that prevents the Commission from exercising general jurisdiction over telecommunications "common carriers."

The idea of creating a level playing field is appealing, particularly when some communications services fall within the jurisdiction of the FTC. In particular, lifting the restriction in certain areas—such as billing, advertising and telemarketing—could ensure that the agency with the most expertise in these areas is taking a leading role.

However, rescinding the exemption completely could lead to duplication of government regulation and/or confusion for consumers in certain areas. For example, telecommunications companies are already subject to the Customer Proprietary Network Information (CPNI) rules administered by the Federal Communications Commission, which limit reuse and disclosure of information about individuals' use of

---

[16] *http://www.ftc.gov/bcp/workshops/infomktplace/index.html*.

[17] CDT has worked closely with the Internet Education Foundation in the further development of GetNetWise—*http://www.getnetwise.org*—which we hope will serve as part of an educational clearinghouse on child protection, privacy and security issues and technologies. The FTC has been the single most helpful government agency in the promotion of GetNetWise.

[18] Alan Westin. Privacy and Freedom (New York: Atheneum, 1967) 7.

[19] *http://www.ftc.gov/os/2002/04/sb2201muris.htm*.

the phone system including whom they call, when they call, and other features of their phone service. At this point, we are not sure it would be wise to take this issue away from the FCC. Similar questions may arise with other issues: Which agency would take the lead? By which rules would a complaint about deceptive notice be addressed? How will these decisions be made?

The Commission has been thoughtful in these areas in the past. Before any jurisdictional proposal moves forward the Commission would need to have a detailed examination of the issues and pan for dealing with areas of overlap.

Conclusion

The FTC is to be commended for taking some very laudatory steps to address the serious and widely shared concerns of the American public about privacy. Indeed, as the foregoing review of issues demonstrates, the FTC already has sufficient expertise to take on general privacy protection responsibilities. However, the Commission has, in our view, taken an unduly narrow view of its jurisdiction, such that Congressional action is needed to establish a baseline of fair information practices in law. We will continue to work with this Committee and the Commission to find innovative, effective and balanced solutions to the privacy problems posed by the digital age.

Senator BROWNBACK [presiding]. Thank you very much for testifying.

I want to thank the entire panel, and the earlier one. I, unfortunately, had some other commitments, so I was not able to be here for much of your testimony, nor of the FTC Commissioners coming in.

I do have a couple of points that I would like to make and some questions that I would like to raise, briefly. This is not for any of the panel members, although it is an issue that I worked with the FTC on closely. It is an investigation on marketing practices of the entertainment industry toward children—marketing violence to children by the entertainment industry.

And I just wanted to compliment the FTC on what I thought was an extraordinary study, and it had a real impact in the marketplace, of entertainment companies that were rating entertainment products for adults and then direct-target marketing it to children. And they did two studies, the original study and then a follow-on, that found this practice widespread, blatant; that, in some movies, R-rated movies, that they were recruiting children as young as nine in the screening of it, in the early marketing phase. They would figure out, "How do we get nine-, ten-, eleven-year-olds to go to this mature movie, or R-rated movie?" And it was a deplorable practice.

But what it did is, it started to change the industry, saying, "OK, you caught us." And everybody—except the recording industry, I would note, if anybody is here from the recording industry, did not amend its practices, and still did not in the follow-on study, either. But I really want to compliment the FTC for taking that issue very seriously, and seriously for the society, and having a major impact of the change, overall.

Ms. Deutsch, I would like to ask you an issue that is somewhat off the mark on FTC reauthorization but is a current issue. And it is in the media now, so I want to get it—I would like—and take advantage of your expertise and knowledge—is the Verizon case with RIAA on privacy on the Internet. We passed a law—oh, gosh, is that last year—Millennium Copyright Act, and it has been interpreted by the courts. And this is one of the first—I believe it is the first case, really, to interpret this. There is a strong concern about the privacy issues involved here.

And I realize you are representing Verizon, so you have a particular point of view on it, but I would like for you to identify what the issues are in that privacy case, because it may be something that comes back up in front of this Committee or in front of the Congress on a case that is between—of trying to balance this issue between privacy and protection of copyrights of intellectual property.

Could you give us a bit of a background and narrow in on the issue involved in that case?

Ms. DEUTSCH. Yes, sure.

This case involves Section——

Senator BROWNBACK. Pull that microphone up a little closer, please.

Ms. DEUTSCH. Sorry.

The case involves Section 512(h) of the Digital Millennium Copyright Act, which governs when can a copyright owner subpoena someone's identity. And it was the service provider's understanding, when we negotiated this law back in 1998, that they could only use this process when the person's identity they were seeking had material that actually resided on our system or network, so we would have someplace to look. If we saw that the material was there, it looked like it was copyright infringement, the subpoena would be valid.

But with the growth of the Internet and peer-to-peer file sharing, the copyright owners, in our view, have tried to stretch an old law to fix a new business problem in a very inappropriate manner. They want the right to use this subpoena process to get access to anyone's identity for conduct that does not occur on our network, but on the user's home computer.

All they need to do is fill out a one-page form. If the form is filled out correctly, they give it to the clerk of the court, who is just a ministerial employee, not a judge. There is no requirement to file a lawsuit or prove you have a registered copyright, or even prove the merits of your case. If the one-page form is filled out correctly, the clerk of the court will stamp that subpoena and then give it to the service provider, and no one in the process has discretion. At that point, we turn over the name of the Internet user.

And we are very worried that not only the recording industry, but because anyone can be a copyright owner, there will be a lot of misuses of the process—by copyright owners, by people who just want your identity for purposes of identity theft or to stalk you or to harm you in some manner. And we do not want to wait until something terrible happens to consumers. We want to fix the problem now, if possible.

Senator BROWNBACK. How many—I am working on a bill on this issue. I am really trying to hit the balance, which is tough to do, to protect that copyright—protection of intellectual property, but also privacy. How many of these subpoenas has Verizon received? Do you know?

Ms. DEUTSCH. Before the recording industry suit, we really only received a handful of subpoenas. No one was using it. But they began a test case, and so we received four from the recording industry for materials off our network.

In 2001, we did receive a subpoena from a copyright bounty hunter, called Copyright.net. They sought, in a single subpoena, the identities of nearly 240 of our subscribers, and they sent the same subpoena to UUNET, seeking almost 3,000 subscribers' identities in a single subpoena. And at that time, we wrote to them and said, "This is invalid," and it went away.

But our concern is that we will be receiving an avalanche of subpoenas from, again, the entire population, seeking people's identity, and we will have no way to know whether the subpoenas are valid or not.

Senator BROWNBACK. What do you mean a "bounty"—you said "bounty hunter"?

Ms. DEUTSCH. Yes, the copyright community hires—I guess you could call them—we call them "third-party bounty hunters." They are companies who work for the copyright community using Internet search bots that scour the Internet for file names that match the names of the copyrighted works, and they send, electronically, millions of notices to the service providers. And because of the volume that we are talking about, and the lack of due diligence, the bounty hunters make mistakes.

Senator BROWNBACK. I was not familiar with that practice.

I am hopeful this is an issue that the Congress can review, again, to try to hit this balance, but also to protect the privacy of legitimate uses, and not encourage, sort of, bounty-hunter type of practices to take place, as well.

I want to thank the panel. As you were going through—I do not know if anybody had a comment that they wanted to make in response to any of the other panel members, but, just before we close, I would like to open that opportunity up to any panel members, if they did have one.

Ms. Grant?

Ms. GRANT. I just want to say that the National Consumers League has signed on to a brief in support of the Verizon issue in that case. We think it is very important.

Senator BROWNBACK. Thank you.

Mr. ROTENBERG. Senator, I wanted to make to mention that I was involved in the amendments to the Federal Wiretap Statute to provide privacy protection for Internet users in the mid-1980s. And I also testified in the House in the late 1990s, when the Digital Millennium Copyright Act was then under consideration. And I warned that Committee that that statute was going to create some new privacy problems for users and also create very difficult problems for the communications industry.

So I just wanted to say that I think your efforts on this issue are very important and also actually quite consistent with the efforts of Congress to safeguard privacy in the communications environment. Without that, without that assurance of privacy protection, I think there are going to be some real problems for all parties.

Senator BROWNBACK. Mr. Rotenberg, where you have worked on this previously, with the Verizon case going against the RIAA case, versus Verizon going against Verizon, where do you see this heading now, then, where there seems to be a court declaration supporting this sort of process?

Mr. ROTENBERG. Well, sir, actually I think your efforts right here in the Senate are the critical next step. Because while I disagree with the judge's determination in that case, I think it has to be made clear to the courts that it really was not the intent of the Congress that it would be so easy, under the DMCA, to use a mere subpoena to get access to information about millions of users. This was—you know, if you go back through the legislative history and also through the Federal Wiretap Amendments, it was clear that there were supposed to be much higher standards.

As you said, sir, you clearly need to enforce copyright laws. You do not want people to be able to escape prosecution when that prosecution is appropriate. But in the structure of the Federal Wiretap Statute, you want to be certain that, when those prosecutions go forward, it is not on the mere whim of a subpoena, as Ms. Deutsch described.

Senator BROWNBACK. Well, I would hope that the industry, that the intellectual-property industry, that is putting this forward, much of it in the entertainment industry and other places, would certainly understand the needs for privacy and the really tough situation we put people in if you start subjecting them to privacy concerns, and on hundreds and thousands of inquiries over the Internet. I cannot think that the entertainment industry would be very excited about a lot of searches like that going out over the Internet to different individuals.

Hopefully, we are going to be able to work together to try to get this resolved, because I certainly do not think the consumer is going to like the notice, or this notion, of these being—hundreds and thousands of these inquiries and searches going out, and bounty hunters in the process.

I want to thank the panel very much for coming in. And I express my appreciation to past work that I have had with the FTC.

The record will remain open for the requisite number of days for the answering of questions that may be submitted.

We do appreciate your participation.

The hearing is adjourned.

[Whereupon, at 5:08 p.m., the hearing was adjourned.]

APPENDIX

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

I thank the Chair for holding today's reauthorization hearing, as the Federal Trade Commission has been the centerpiece of numerous recent policy discussions. Given the heightened attention to the high tech sector in particular, it is fitting that we examine the role that the FTC plays today and may play in the future. This reauthorization hearing will allow us to focus on several issues, but the most important in my view are the requests by the FTC for common carrier jurisdiction and a grant of rulemaking over "abusive and deceptive" practices concerning spam.

The request put forward by the FTC for common carrier jurisdiction strikes me as misguided and over-reaching. I agree with the well-reasoned, commonsense position of FCC Consumer Affairs Bureau Chief Snowden, who in a recent letter to the FTC indicated that the FCC has far greater resources available to deal with common carrier issues and also a greater scope for enforcement. For example, if the FCC takes action against a common carrier it may revoke licenses, unlike the FTC.

While the Commissions should work together for the benefit of the consumer, I simply do not believe that having two Federal agencies performing essentially the same core functions is effective. Rather, I am supportive of the idea of a Memorandum of Understanding between the Commissions that would clarify the role of each agency to prevent the inefficiencies and duplication of work which inevitably arise from overlapping jurisdictions.

I also want to discuss a topic which is of great concern to me, the spiraling problem of spam. This volume of this "digital dreck" has become so overwhelming that it is expected to overtake regular e-mail this very summer. While I am pleased that the FTC has been addressing spam, including holding a very productive Spam Forum recently, I am troubled by the direction the Commission has taken in its testimony today.

Rather than a broad grant of rulemaking over "abusive and deceptive" practices as exists in the FTC's telemarketing authority, I believe that the best way to proceed in this area is with specific requirements set forth by the Congress. Senator Wyden and I have been working on antispamming legislation for several years now and in fact the CAN–SPAM bill is scheduled for the June 19 markup in the Committee. We have been working to identify appropriate guidelines for legitimate businesses and strong enforcement tools to combat bad actors and I am confident that the right balance has been struck in the CAN–SPAM bill. While focused rulemaking may provide assistance by following specific provisions set forth by the Congress, I am extremely wary of wide grants of vague additional authority.

I value the expertise of the Commission and look forward to working with it on both technical and legal ways to resolve the increasingly damaging problem of spam. Thank you.

○