AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CHALLENGES FACING THE FEDERAL TRADE COMMISSION

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

NOVEMBER 7, 2001

Serial No. 107–68

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

76–308CC WASHINGTON : 2001

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

	Page
Testimony of:	
Muris, Hon. Timothy J., Chairman, Federal Trade Commission	10
Material submitted for the record by:	
Business Roundtable, The, report entitled Information Privacy: The Current Legal Regime	40
Davis, Anna, Office of the Director, Congressional Relations, Federal Trade Commission, letter dated December 5, 2001, to Hon. Clif Stearns, enclosing response for the record	35
Simons, Joseph J., Director, Bureau of Competition, Federal Trade Commission, letter dated December 3, 2001, to Hon. Edward Markey, enclosing response for the record	38

CHALLENGES FACING THE FEDERAL TRADE COMMISSION

WEDNESDAY, NOVEMBER 7, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:08 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Deal, Whitfield, Shimkus, Bryant, Buyer, Terry, Bass, Tauzin (ex officio), Towns, Markey, Eshoo, and Dingell (ex officio).

Staff present: Ramsen Betfarhad, majority counsel; Kelly Zerzan, majority counsel; Brendan Williams, legislative clerk; Jonathan Cordone, minority counsel; and Bruce Gwinn, minority professional staff.

Mr. STEARNS. Good morning. The subcommittee will come to order. I welcome all of you, especially our witness, the Chairman of the Federal Trade Commission, Mr. Muris. I am pleased to have you today and look forward to your testimony.

I hope that your testimony today would be one of many before the subcommittee during your tenure as Chairman of the Commission. As a committee of jurisdiction with oversight responsibilities over the Commission, I find it important that there be good lines of communication between the committee and the Commission.

I consider both our oversight obligations and our mandate to protect consumers to be of utmost import, and therefore week a close working relationship with the Commission.

I hope that all subcommittee members will take the time to visit with the Chairman, and the other members of the Federal Trade Commission.

I understand that your testimony today is on behalf of the Commission, and that it will outline the Commission's agenda, and specifically it is enforcement and programmatic priorities.

I commend you and the Commission for focusing on the fundamentals which in the case of an enforcement agency, such as the FTC, is a vigorous enforcement of the existing laws. I also share with the Commission a keen interest in a number of other matters identified in your testimony as being priority issues for the Commission.

One of these issues, of course, is privacy. As you are aware, and as we have talked about, our committee has held six hearings on

this matter, and we have amassed a great deal of information on this subject, and we think our hearings have been instrumental in a better understanding of the issue.

I welcome your attempt at focusing the Commission's resources on enforcement, and as you have mentioned, specifically enforcing existing laws that either directly or indirectly have privacy implications. That is after all precisely what an enforcement agency should be doing, enforcing the law.

As was evident by the subcommittee's May hearing on cyber-fraud and crime, I and many other members of the subcommittee find cyber-fraud and crime to be particularly important and worthy of special attention by the Commission.

The potential for such fraudulent and criminal activities to impact thousands of consumers, and engender great financial losses make them particularly troubling. The FTC's consumer sentinel, Depository of Cyber-Fraud Complaints Accessible to Law Enforcement Agencies, is an important step.

Nevertheless, effective law enforcement actions against cyber-fraud crime I think requires greater participation by both human and artificial intelligence. Moreover, the record from our hearing in May suggested less than a stellar level of cooperation between the various enforcement agencies when confronting cyber-fraud and crime.

If such problems persist today, let us know. There is no excuse for interagency turf issues impending or undermining effective identification and prosecution of fraudulent and criminal activities on-line or off-line. I also welcome the Commission's commitment to a more aggressive enforcement and education initiative targeting health care fraud, and in particular, deceptive and misleading health claims.

Health fraud is especially repugnant, as it impacts members of our society that are among the more vulnerable, such as the elderly and the young. And health fraud impacts the life and physical well-being of the American consumer, something much more important than just his or her pocket book.

The Commission faces an arduous task combating health fraud, one that was made more difficult with the advent and proliferation of health websites. Also, taking a cue from your testimony, I also want to highlight my interest in two other issues.

First, I think that increasingly the intersection between intellectual property rights and anti-trust law is being colored by flux or tension, and as such it requires greater vigilance on the part of our anti-trust enforcers.

Moreover, I think we have just begun to understand and grapple with the significance of standards and standard setting organizations, as key sectors of our economy now are subject to network effects.

I commend the Commission for their focus and attention on these two matters. Moreover, we are in agreement that consumer education is a critical mission of the Commission. I do believe that empowering the American consumer with knowledge is a most effective and potent consumer protection.

I would encourage you and the Commission to explore new and creative ways of informing the American public of your work. I

know very few people that are aware of the good work that the Commission undertakes on behalf of the American consumer.

Let's make a concerted effort to change that. One thought that I had was for the Commission to use banner ads to inform the American public about its various activities, or alert them, just simply alert them, to the various scams. Just a thought.

And finally I would be remiss if I didn't raise an issue that I, and I believe many Americans, find important today. First and foremost, I would appreciate your comments as to whether the FTC has any evidence of fraud being perpetrated against the Americans using charitable giving for the September 11 victims as a pretext.

Second, I would like to know whether the Commission has any persuasive authority with legitimate charitable organizations convincing them—convincing them—to disperse all the money collected for September 11 victims to those victims' families in a timely manner.

We had an oversight hearing on this yesterday, in which it was evident that a lot of these charities were accumulating large sums of money and were very slow in dispersing it. I thank you for your testimony today. I am glad that we are able to do it in this room.

Unfortunately, we had to cancel the previous hearings, and I appreciate your patience, and I am glad that you are here today, and I look forward to working with you, and my colleagues and I know that we are going to have a great relationship with you during the 107th Congress.

And with that, I will close, and ask the ranking member, Mr. Towns, the gentleman from New York, for his opening statement.

Mr. TOWNS. Thank you very much, Mr. Stearns. I would like to welcome the Chairman to the committee, and look forward to his testimony. The Federal Trade Commission has always played a pivotal role in America, standing with consumers and representing them against commercial interests, and who do not always have the customers' best interests in mind.

And so I am pleased to have the new Chairman before us today, and having met with the Chairman a few weeks ago, I have all the confidence in the world that you, Mr. Chairman, will stand up for the consumers on every possible opportunity.

Having said that, there are some issues of concern that I would like to see addressed today at the hearing. I would hope that you would address what seems to be a never-ending list of mergers which sits before the Commission and the issue of consumer privacy in both on-line and off-line situations.

I know that you, Mr. Chairman, have every intention of being open about the happenings at the Commission through your testimony, and of course through your answers to our questions as well.

I look forward to working very closely with you in the days and months ahead, and on that note, Mr. Chairman, I yield back the balance of my time.

Mr. STEARNS. I thank the gentleman, and recognize Mr. Shimkus for an opening statement.

Mr. SHIMKUS. Thank you, Mr. Chairman. I do want to welcome the Federal Trade Commission Commissioner here, Mr. Muris, and I want to focus my short comments and listening to the debate on a couple of issues. And one was from my colleague on the merger

issue, but the focus that I have had since I have been involved with the NATO parliamentary assemble and the EU issue is the usability to deny mergers that in essence we have approved here.

And in essence the competitive disadvantage placed upon the United States and a lot of our fine companies because of the EU application process, and then the barriers that they are able to drop without—well, in essence, in negotiation, and we are at a competitive disadvantage.

The other issue that I will address in the question and answer period is on the Internet and some patrolling of some of the business opportunities offered there, and the role in which you play.

And I still have not—we know in the Department of Ag the Packers and Stockyard Act is the vertical integration aspect of merging concentration, and I am wondering where the line is drawn when it goes into the corporate application of the boxings of food and material. I know that is a big concern in the agricultural sector, is the concentration of that market in the hands of a few, leaving the producers at the whims of only a handful of purchasers.

It is probably not in our venue. It is of my concern, and those are the things that I will be listening for and going into during questions and answers. Thank you, Mr. Chairman, and I yield back my time.

Mr. STEARNS. I thank the gentleman and recognize the gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman, and welcome, Mr. Chairman, to your first meeting here with the Commerce Committee. The FTC recently announced that it was no longer going to recommend that Congress pass a law to protect the privacy and freedom of Americans on the Internet.

Instead, the Agency announced that it would attempt yet again to get more of the on-line industry to take voluntary actions to protect personal privacy comprehensively. The Commission also indicated that it would renew its commitment toward stepping up its enforcement actions.

I salute the laudable efforts of certain segments of the industry in trying to develop so-called self-regulatory solutions to some of the privacy concerns that many have expressed.

These undertakings are critical to increasing consumer confidence and trust in the medium, and will be an important component in any comprehensive set of privacy protections for our consumers.

Relying solely upon voluntary industry efforts, however, will not suffice. I believe that the progress that has been made in part voluntarily must be coupled with comprehensive protections for all Americans. There is no reason to delay in developing standards for such privacy protection.

I do not accept the notion that the Internet is too complex and technology changing too rapidly to develop enforceable privacy protections for our consumers. As technologies change and business plans for on-line commerce adjust, consumers' privacy protections remain a constant.

Again, consumers can negotiate in the marketplace for better privacy protection if they can get it, but no consumer should be with-

out basic privacy protections, or without recourse to redress grievances for harm caused by privacy invasions.

With respect to enforcement, increasing agency activity on this front is certainly welcome. Efforts can be made to protect Americans through enforcement, for example, of the law that we passed to protect the privacy of children on the on-line environment, as well as existing telemarketing laws.

I authored the law which was approved by this committee 10 years ago to establish do not call telemarketing rules to protect consumers. That law also permitted regulators in Section 227 of the Communications Act to establish a national do not call data base, rather than company by company lists which drives people crazy.

At the time the FCC chose not to endorse a data base technology, although authority to implement it still exists on the books today. I encourage the Federal Trade Commission to step up its enforcement of the current do not call regulations and explore how technology from the private sector can help protect consumers today.

In addition, Mr. Chairman, my hope is that the FTC will increase its investigation and analysis of products purported to be secure for consumer use, especially when such on-line use may include sensitive personal data.

In this regard, enhancing the FTC's role in protecting consumers from security risks and new software products, and on-line services such as those alleged by consumer groups to be inherent in Microsoft's new Windows XP Operating System, and its Passport Program, is also something that I believe the FTC must explore in a timely fashion.

I would argue that the Federal Trade Commission should begin its inquiry almost immediately since this product has the potential of compromising consumers and I believe that we shouldn't wait until after the damage is done to millions of Americans before there is an inquiry which is announced, and which may in and of itself be enough to protect consumers.

Increased enforcement, however, will not help anybody if the egregious conduct is not yet against the law, and that is why I continue to believe that we must pass on-line privacy legislation.

I thank the chairman for calling the hearing, and I look forward to working with you, Mr. Chairman, and again we welcome you to our greatest of all committees in Congress. It is great to have you with us.

Mr. STEARNS. Thank you. The Chair recognizes Mr. Buyer for an opening statement.

Mr. BUYER. Mr. Chairman and Mr. Towns, I want to thank you for inviting the Chairman to come up and see us. Mr. Chairman, I have—I may not be able to be here for the question phase, and so I just want to let you know some areas of interest that I have.

I note that in your testimony that you touched on five areas, and I join Mr. Shimkus with a concern about vertical integration in agriculture, and I noticed in your testimony that you had mentioned that you had wanted to follow the guidelines with regard to—you said that the Agency will continue to follow the merger guidelines when assessing the impact of the proposed merger on competition.

And then you cite horizontal guidelines, and I don't know about how you handle vertical integration, but I do know that farmers out there today have less choices, less choices where they buy their equipment, and where they get their Ag inputs, and even limit on their markets.

And it is very concerning what is happening out there in the Ag world. I also have concerns with regard to—there is a bill here in Congress called the Franchise E Act. It is a concern between the franchise owners and the parent companies, and it is a very serious issue, and it is one that we need to look at.

The issue on—and one that I have never been able to figure out in the 9 years that I have been in Congress, is multi-level pricing in drug companies. I think the day that I can figure out how they do pricing in airline tickets, I will be able to figure out how they do multi-level prices in with drug companies.

Another issue of concern that I have on consumer protection deals with sports programming. What is occurring today is with baseball as an example, and Congress gives baseball an anti-trust exemption. The baseball owners then pay these outrageous salaries to athletes.

And they pay $250 million to a shortstop, and people go how can an owner do that. An owner can do that because he takes those costs and passes them off to the programmers, and then people don't know why their cable rates are going up.

They think cable rates are going up, Mr. Chairman, because of infrastructure upgrades. Cable rates are going up because sports programmers are taking advantage of consumers all across the country, and that is something that really concerns me.

And it is a conversation that I want to continue to have with you, and as a matter of policy, and before I yield back my time, before I was on the Judiciary Committee for 4 years, and would work with the anti-trust division of the Department of Justice, I was really concerned about the level of merger mania that occurred there in the 1990's.

And something bigger is better and can provide greater efficiencies, and therefore the consumer gets something at a lesser cost. Wait a minute. Time out. Aren't we about protecting the small businesses and the entrepreneurs so that we have an open and fair competitive marketplace?

I think that is what the job of government should be in a capitalistic economic system. So as a matter of policy, I look forward to your comments on how a new administration views the world and the marketplace. I yield back and thank you for my opening comments.

Mr. STEARNS. I thank the gentleman, and the Chair recognizes the distinguished ranking member of the full committee, Mr. Dingell.

Mr. DINGELL. Mr. Chairman, I thank you. I thank you for holding the hearing, and I believe that it is an important one on a very important subject. The issues facing the Federal Trade Commission during these uncertain times are a matter of great concern, and I look forward to hearing the views of the Commission's new Chairman.

One issue that I am particularly concerned about is the growing problem of identity theft, especially in the wake of the terrifying events of September 11. Within the limitations of its current resources and authority, I believe the FTC has made some progress in addressing fraud perpetrated through the use of stolen identities. I applaud these efforts.

But we will have to see whether they are sufficient and I believe that there is evidence developing that they are not. We now live in a new reality, a reality in which the production and use of false identifications have very clear implications, and not just for ordinary citizens, but for the very security of the Nation itself.

It's not just our personal financial security at stake. We once were only concerned with stolen identities, aiding thieves and con artists. Now we must be concerned with stolen identities aiding terrorists, and allowing them to conduct activities anonymously, and potentially granting them access to secure locations.

The Commission must conduct a thorough examination of who has access to personally identifiable information in commerce, and the processes by which such information is collected and disseminated.

The collection and transfer of non-public information has become an industry in and of itself, and it is used now to enrich people, and very frankly to hurt the people whose personal information is being used.

For a fee today intimate and personal detailed information can be obtained by and about virtually anybody or everybody. The genie of privacy has been released from the bottle, and we are left with an extremely difficult task of putting it back in.

Existing laws and government resources simply cannot restrict broad access to personal information of consumers. Years after the murder of Amy Boyer, Congress has still not prohibited the unauthorized sale or transfer of Social Security numbers that played such an important role in that case.

Alone, neither industry self-regulation nor the government can fully protect the public against identity theft, and indeed I would note that industry has shown very little concern or interest in protecting the identities and the personal privacy of American citizens.

Indeed, the most effective weapon against identity theft is to empower consumers with control over their personal information, and how that information is collected and disseminated.

If citizens are armed with effective, and enforceable, legal rights, then the individual consumer should be able to manage access to his or her personally identifiable information more responsibly than industry or government.

In conclusion, I agree with Chairman Muris that Congress should not limit new privacy legislation to on-line practices. Our goal must continue to be consumer control over their personal information, whether on or off-line, or indeed wherever it might happen to be.

Under your leadership, Mr. Chairman, we expect the FTC to assist us in this endeavor. If we fail in this critically important task, we should expect the States to address the problem in ways that will pose far more problems for industry than any new Federal law.

Indeed, the States could give us 50 or more different solutions to a problem, which might create significant problems for industry if industry does not recognize that situation.

So industry, like individual Americans, then has a strong interest in seeing effective, enforceable, new authority and rights enacted. We must stop identity theft and we must do it now. We must see to it that the privacy of the American people is protected for new reasons above and beyond those which Mr. Markey and others on this committee and I have traditionally pushed.

Mr. Chairman, I look forward to working with you on this important matter, and I welcome Mr. Muris for his appearance before this committee. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Mr. Terry is recognized for an opening statement.

Mr. TERRY. Thank you. I just want to thank the Chairman for being here today, and I am anxious to hear your vision and your philosophy for the department under your leadership; and I also want to express my appreciation for your attempts to see each of us individually.

That impressed me, and what also impressed me is how you are going to get your arms around so many important issues. Just listening to the opening statements today, each one of us have different concerns, of which have incredible significance and magnitude to them, and I am particularly going to listen in as Mr. Boyer mentioned on vertical integration in foreign policy.

But I am going to look at it and attack the issues, and see when an Internet company is allowed to just control all of the transactions, or how we allow more small tech businesses to be involved in the process. So with that telegraph of where I will ask my questions, I will yield back the rest of my time.

Mr. STEARNS. I thank the gentleman, and the Chair recognizes the gentleman from New Hampshire, Mr. Bass.

Mr. BASS. Thank you, Mr. Chairman, and I appreciate also you holding this hearing. The Federal Trade Commission is more than perhaps any regulatory agency the heart of the jurisdiction of this committee besides Energy. I mean, Commerce is trade, and we want to welcome the new Chairman.

There are many issues that we need to review and address over the coming years, including issues such as identity theft, privacy, anti-trust, and oversight, and other consumer protection issues. So I think this is a great opportunity to get an introduction, and we will be discussing many important issues today, and I thank the chairman for holding the hearing.

Mr. STEARNS. I thank the gentleman.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. ED BRYANT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

I would like to thank Chairman Muris for testifying before us today about the challenges facing the Federal Trade Commission. I look forward to hearing from the Chairman on the Commission's work protecting the welfare of our nation's consumers.

As the chairman discusses in his testimony, the FTC is the only federal agency with jurisdiction across many sectors of the nations economy in the areas of both consumer protection and competition. I am particularly interested in hearing from

the Chairman on the Commission's work in regard to technology and intellectual property, health care, privacy, energy, and mergers.

It is important that the FTC continues to fight Internet and health care fraud and educate consumers about the characteristics of scams so that the nation has educated and aware consumers.

I understand that many on the Commission do not believe there is a need for Congressional action in regard to information privacy—I hope to hear from the chairman on the reasons why some commissioners have concerns about action in this area.

I consistently hear from a number of my constituents regarding the deluge of unsolicited emails they receive, and I am glad to hear that the FTC has an electronic mailbox where consumers can forward their spam.

I also look forward to hearing about the Commission's work looking out for the interests of the consumers in its evaluation of mergers.

I thank the Chairman for holding this hearing today and again, thank Chairman Muris for testifying before us today on the agency's work to protect the welfare of consumers.

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Let me thank you, Mr. Chairman, for calling this morning's hearing, which promises to provide us an excellent opportunity to discuss various challenges facing the FTC.

This hearing will allow us to look forward a bit, to see what may be just over the horizon and how the federal agency charged with consumer protection plans to confront them. So I am pleased, as well, to welcome our distinguished guest, Federal Trade Commission Chairman Tim Muris.

Given its general statutory authority to protect consumers from unfair or deceptive acts or practices, the FTC serves as consumers' principal federal guardian in the marketplace. From its policing of Internet fraud to generic drugs, to gas prices, the FTC helps to ensure the competition and honest dealing that is necessary for markets to thrive. And as the former head of the Bureau of Consumer Protection, Chairman Muris—I am sure—fully understands the scope of the public trust he now holds.

Over the past few years, the FTC has also made its mark on the Internet age, as the body in charge of approving mega-mergers, such as the union of AOL and Time Warner, of establishing online anti-fraud guidelines, and providing safeguards to protect the Internet users' personal information. The future, doubtless, will contain many of the same debates.

Privacy, for instance, is one issue that has been actively debated in this Subcommittee and I look forward to more discussion on that front this morning. I commend Chairman Muris for his thoughtful examination of this complex issue, as demonstrated by his recent speech in Cleveland, which focused on rededicating the FTC's attention and resources to enforcement issues, specifically actions related to consumer privacy. Chairman Muris' focus on enforcement is right on target.

Although it is unlikely the Committee will have time to tackle the issue this year, given the shrinking session, I do see a need to explore additional legislative efforts that will help address an apparent failure in the marketplace to protect consumers' privacy. Perhaps there are some additional tools we can provide that will bring confidence to consumers and the industry without unnecessarily interfering with good business practices.

Finally, Chairman Muris has long argued, and I agree with him, that the Commission should evaluate the economic impact of its actions closely and make sure that any proposed action will benefit consumers. The Commission should take aggressive law enforcement actions against fraud and deception, but take care to steer clear from cumbersome rule-makings designed to transform entire industries. Consumers benefit tremendously from free markets and competition, and I look forward to continued acknowledgement of this fact at the FTC.

Mr. Chairman, I look forward to the discussion today, and to working with you during your term.

Mr. STEARNS. At this point we welcome the testimony of Timothy Muris, the Chairman of the Federal Trade Commission. I think you have heard from a number of members who have brought up some interesting topics that you probably had not intended to talk about,

such as baseball and the cable companies. But we welcome your testimony this morning.

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

Mr. MURIS. Thank you very much, Mr. Chairman. Let me briefly summarize my testimony and submit my statement for the record.

I am certainly pleased to be here today. It has been a while since I testified before this committee, and this is my first testimony as Chairman of the Federal Trade Commission.

I have been here at the FTC for 5 months. As your questions imply, the FTC has a very broad mandate. It is the only Federal Agency with both consumer protection and competition jurisdiction in broad sectors of the economy.

This is the fourth job that I have had at the FTC, and I am honored to be Chairman. Our mission is important, as your questions have indicated. The issues are crucial and fascinating, and the people with whom I work are outstanding public servants.

I am especially pleased to appear before this subcommittee for my first Congressional testimony as chairman. The committee and its chairman have been good friends to the FTC, and I especially benefited from the chairman's leadership on privacy. Privacy was a new issue for me, and I learned much from this committee's six hearings on the issue. The facts from those hearings led to our new privacy agenda, including increasing our resources devoted to protecting privacy by 50 percent.

The FTC's record is impressive, and unlike the 1980's when I was last at the FTC, the FTC today is an example of bipartisan cooperation. We will continue the excellent work of our predecessors—my friend Bob Pitofsky and his colleagues.

Let me briefly discuss our two major missions, consumer protection and anti-trust. In consumer protection, 20 years ago the FTC shifted from an attempt to be the second most powerful legislature in Washington, to enforcing basic consumer protection laws: laws against fraud, against deception, and against breach of contract. In the 1990's, this mission was perfected and performed extremely well using a three-part strategy of law enforcement, of consumer education, and of cooperation and working with the business community.

Today the FTC is the leader both in fighting fraud on the Internet and in using hi-tech tools to detect and deter fraud and educate consumers about on-line scams. Last month, for example, we obtained an injunction against a cyber-scammer who allegedly used more than 5,500 copycat web addresses to divert consumers from their intended destinations to one of his sites, and then hold them captive while pelting them with a barrage of advertisements, many of them for products such as pornography, which many consumers regard as inappropriate.

Another recent example is that we announced a settlement in a negative option case with more than $8 million in redress for consumers. We also recently announced eight diet supplement cases, which is an area in which we have seen an increasing number of problems.

Following September 11, we have turned our attention to many potential scams. We have recently worked with law enforcement officials all over the country to search the Internet for potentially fraudulent and deceptive claims related to terrorism issues, and we have numerous investigations underway. We have also launched an aggressive consumer education campaign, warning consumers what to look for in potential scams and also addressing the charitable solicitation issue. We finally have been screening, along with many other agencies, for fraudulent charitable solicitations.

Turning to anti-trust, the watch word again is continuity. The merger wave was extremely significant in the late 1990's, and it has receded somewhat, but we are still vigilant on the merger front.

Last month, for example, we brought four merger cases. On nonmergers, we are increasing our efforts, particularly in health care. Health care costs as you know compromise about 15 percent of our GDP, up from 12 percent just 10 years ago. Not surprisingly, health care cases are an important part of our focus. In particular, we are increasing our efforts to prevent firms from engaging in anti-competitive practices that raise drug prices.

We have investigated claims that manufacturers use the provisions of the Hatch-Waxman Act anti-competitively. One problem involves agreements between makers of brand-name drugs and makers of generics, under which the generic entrant is essentially paid not to compete. A second issue under Hatch-Waxman involves efforts unilaterally by brand manufacturers to forestall competition, and we are looking hard at that area as well.

In summary, and I did want to briefly summarize my statement and allow you to turn to your questions, our mission is simply to protect consumers. Today's FTC has forged a widespread and bipartisan consensus on how to protect consumers, and how to work with other Federal and State agencies to provide maximum benefits. We will continue to use the full panoply of our institutional tools in fulfilling this important mission.

Thank you very much.

[The prepared statement of Hon. Timothy J. Muris follows:]

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

Mr. Chairman and Members of the Subcommittee, I am Timothy J. Muris, Chairman of the Federal Trade Commission. I am pleased to appear before you today on behalf of the Commission to discuss our law enforcement and programmatic priorities.[1]

The FTC is the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy.[2] We enforce laws that prohibit business practices that are anticompetitive, deceptive, or unfair to consumers, as well as promote informed consumer choice and public understanding of the competitive process. The work of the FTC is critical in protecting and strengthening free and open markets in the United States.

---

[1] The written statement presents the views of the Commission. My oral statement and responses to questions are my own and do not necessarily represent the views of the Commission or any other individual Commissioner.

[2] The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.* The statute provides the agency with jurisdiction over most of the economy. Certain entities, such as depository institutions and common carriers, are wholly or partially exempt from FTC jurisdiction, as is the business of insurance. In addition to the FTC Act, the FTC has enforcement responsibilities under more than 40 statutes.

The FTC's record is impressive. The agency has fulfilled its mission of protecting American consumers by pursuing an aggressive law enforcement program during rapid changes in the marketplace—the past decade saw the largest merger wave in history, the rapid growth of technology, and the increasing globalization of the economy. Through the efforts of a dedicated and professional staff, the FTC has shouldered an increasing workload despite only modest increases in resources. We also have benefitted greatly from the leadership of my predecessor, Robert Pitofsky.

The guiding word at the FTC will be "continuity." The agency aggressively will pursue law enforcement initiatives, launch consumer and business education campaigns, and organize forums to study and understand the changing marketplace, just as it has done for several years. We will continue to address competition and consumer protection issues in the evolving economy with the same expertise and commitment as before.

Our competition mission will continue to reflect the following widely shared consensus: (1) the purpose of antitrust is to protect consumers; (2) the mainstays of antitrust enforcement are horizontal cases—cases involving the business relations and activities of competitors; (3) in light of recent judicial decisions and economic learning, appropriate monopolization and vertical cases are an important part of the antitrust agenda; and (4) case selection should be determined by the impact on consumers, guided by sound economic and legal analysis, and made with careful attention to the facts. The FTC is primarily a law enforcement agency, and we will continue aggressive enforcement of the antitrust laws within the agency's jurisdiction. The FTC is also an independent expert agency and a deliberative body, and is thus well suited to studying an evolving marketplace and developing antitrust policy—we will continue to hold public hearings, conduct studies, and issue reports to Congress and the public.

Similarly, there is widespread agreement on how the FTC best carries out its consumer protection mission. Twenty years ago, the FTC shifted its emphasis toward more aggressive enforcement of the basic laws of consumer protection. The staple of our consumer protection mission is to identify and fight fraud and deception. The Commission continually monitors trends and developing issues in the marketplace to determine the most effective use of its resources. The FTC has become the national leader in consumer protection and partners with other law enforcement agencies at the federal, state, local, and even international levels to maximize benefits for consumers.

The FTC will continue to address significant law enforcement and policy issues throughout the economy, devoting the major portion of its resources to those areas in which the agency can provide the greatest benefits to consumers. I will highlight five areas today:

- Technology and Intellectual Property
- Health Care
- Privacy
- Energy
- Mergers

TECHNOLOGY AND INTELLECTUAL PROPERTY

Changes in technology and the growing importance of intellectual property to the economy have caused a significant change in the FTC's work in both missions. The consumer protection mission focuses increasingly on high-tech frauds, while the competition mission works to provide consumers with the full benefits of both innovation and competition.

High-tech fraud. The FTC is the leader both in fighting fraud on the Internet and in using high-tech tools to detect and deter fraud and to educate consumers about online scams. The Internet has spawned new deceptive practices, and also has given renewed vigor to traditional scams. The FTC will continue to monitor rapidly evolving technologies used by scam artists. The FTC has brought a number of cases involving scams that depend on the special nature of technology. In a case filed September 25, for example,[3] we obtained an injunction against a cyber-scammer who allegedly used more than 5,500 copycat Web addresses to divert consumers from their intended destinations to one of his sites and hold them captive while pelting their computer screens with a barrage of advertisements.[4]

[3] *See FTC v. Zuccarini,* No. 01-CV-4854 (E.D. Pa. filed Sept. 25, 2001).

[4] This scam involved registering Internet domain names that are misspellings or transpositions of legitimate popular domain names to lure surfers onto a Web site that they never intended to visit. Once taken to the defendant's sites, consumers were "mousetrapped," making it difficult to exit. Mousetrapping involves the use of a special programming code at the site

Traditional frauds have migrated to the Internet in large numbers. Many of the 200 cases challenging Internet fraud brought by the FTC since 1994 concerned old frauds in the new medium—28 cases challenged credit repair schemes, 13 cases challenged deceptive business opportunities, and 11 cases challenged pyramid schemes. The Internet can give these old scams a sleek, new veneer, as well as provide access to a larger pool of potential victims at little cost.

We also use technology in our fight against fraud. Our high-tech undertakings include:

- *Consumer Sentinel*—A consumer complaint database and web-based law enforcement tool that is maintained by the FTC and shared with over 300 law enforcement agencies in the U.S. and abroad. This database is an integral part of our overall consumer complaint system. Analysis of the complaints in the database enables staff to spot trends and identify targets. The database already has been expanded to cover identity theft complaints, and this year will be expanded further to cover additional types of privacy complaints. We are also working with the Department of Defense on Soldier Sentinel, a database tailored to accept consumer complaints from military personnel and to track trends in frauds specifically targeted at members of the armed forces.
- *E-consumer.gov*—A joint effort with 13 other nations launched earlier this year to gather and share cross-border e-commerce complaints.[5]
- *Surf Days*—Joint initiatives whereby the FTC staff identifies a deceptive practice that is prevalent on the Internet and recruits law enforcement partners to fight it. Together we search the Web for a specific period of time using a specially tailored protocol. Surfs can be highly efficient tools that: (1) enable law enforcement officials to learn about online practices; (2) provide an opportunity for the FTC to alert and educate Web site operators—some of whom are new entrepreneurs, unaware of existing laws—whose sites appear to violate the law; and (3) enable law enforcement authorities to identify the more egregious violators for possible law enforcement action.
- *Internet investigation training*—FTC-conducted training for more than 2000 individual law enforcement staff, including representatives of 20 countries, 30 states, and 22 federal agencies. This training will continue.
- *Toll free number*—The FTC's toll-free hotline, 1-877-FTC-HELP. The hotline will receive additional resources to accept more consumer complaints and help us to identify trends in consumer fraud. Complaints received through the hotline are entered into Consumer Sentinel and made available to law enforcement agencies across the country.

Intellectual property. In past decades, our economy has become more knowledge-based; for some companies, patent portfolios represent far more valuable assets than manufacturing or other physical facilities. Thus, an increasing number of the FTC's competition matters require the application of antitrust law to conduct relating to intellectual property. Both antitrust and intellectual property law share the common purposes of promoting innovation and enhancing consumer welfare. On occasion, however, there have been tensions in how to manage the intersection between the doctrines, as well as questions about how best to spur innovation through competition and intellectual property law and policy. These issues may well merit broader and more in-depth study. In addition, we continue to pursue investigations involving intellectual property.

An example of our objectives in this area is to ensure that patent holders do not improperly withhold critical information from industry standard-setting groups to delay the creation of a standard or raise the price of admission to its use. In *Dell Computer,*[6] the FTC considered the issue of the capture of a standard-setting body by a holder of intellectual property rights that were critical to the standard ultimately selected by that body. Dell, a member of a standard-setting association, allegedly had influenced the choice of an industry standard for computer graphics performance without disclosing that its own intellectual property rights would benefit from the adoption of that standard to the detriment of its competitors and, ulti-

---

that obstructs surfers' ability to close their browser or return to the previous page. Clicks on "close" or "back" buttons only cause new unwanted windows to open. The defendant's sites also contained a "stealth" feature, hidden under the task bar, making it invisible to consumers. Its sole function was to act as a timer, periodically launching additional pages of advertisements, without any action by consumers. Thus, even as consumers struggled to escape the defendant's multi-window mousetrapping scheme, they were barraged with even more windows of unwanted images.

[5] The other countries participating in this project are Australia, Canada, Denmark, Finland, Hungary, Japan, Mexico, New Zealand, Norway, South Korea, Sweden, Switzerland, and the United Kingdom.

[6] *Dell Computer Co.,* C-3658 (May 20, 1996) (consent order).

mately, consumers. To settle the FTC's charges of antitrust violations, Dell agreed not to enforce its intellectual property rights. We currently are investigating matters that raise similar issues.

HEALTH CARE

Health care costs comprise a large part of both the family budget and the national economy. Currently, health-related products and services account for approximately 15 percent of gross domestic product, up from 12 percent in 1990. Not surprisingly, health-related cases constitute an important part of the FTC's focus.

Generic drugs. A major portion of the American health care dollar purchases prescription drugs, and we will continue our efforts to prevent firms from engaging in anticompetitive practices that raise drug prices. In particular, we will strive to ensure that anticompetitive practices do not delay market entry of generic drugs, which cost less than name-brand pharmaceuticals. We will seek to ensure that protections provided to drug innovators under the Hatch-Waxman Act[7] are not abused to the detriment of consumers. As you know, Hatch-Waxman was designed to increase the flow of new pharmaceuticals into the marketplace by carefully balancing two public policy objectives: encouraging vigorous competition from generic drugs, while maintaining incentives to invest in the development of innovator drugs.

The FTC has investigated claims that manufacturers use the provisions of this Act anticompetively in two different ways. The first involves agreements between makers of brand-name drugs and makers of generics, under which the generic entrant is essentially paid not to compete. In *Abbott/Geneva,*[8] for example, the parties allegedly agreed that the generic manufacturer—in exchange for money paid by the branded manufacturer—would not enter the market until their patent litigation concluded; would not enter the market with any other generic version of the product; and would not relinquish the 180-day period of exclusivity given to it under Hatch-Waxman as the firm first to file an application to make a generic equivalent.[9] Such agreements may unreasonably delay the entry of generic drug competition, potentially costing consumers hundreds of millions of dollars annually.

The second issue involves unilateral conduct by branded manufacturers designed to forestall competition. For example, some branded manufacturers list additional patents in the FDA's "Orange Book," often shortly before their original patents expire, which sets the stage for launching patent infringement suits against generic drug firms poised to enter the market. Under Hatch-Waxman, such litigation triggers an automatic 30-month stay on FDA approval of the generic drug. If the listings do not meet statutory and regulatory requirements, their inclusion in the Orange Book may constitute unlawful restraints on competition.

To uncover whether strategies such as these are isolated examples or represent patterns of anticompetitive conduct, the Commission has undertaken a study, as requested by Representative Henry Waxman, to provide a more complete picture of how generic competition has developed under the Hatch-Waxman Act. The Commission has issued nearly 100 orders to innovator and generic drug companies to obtain documents related to the issues identified through investigations and to identify any other anticompetitive strategies that may exploit certain Hatch-Waxman provisions. The facts obtained through this study may provide a basis for policy recommendations in this area.

Health care fraud. Fraud in the health care sector poses a direct and immediate threat of both economic and physical injury to consumers.[10] To fight health care fraud, the FTC launched "Operation Cure.All," a comprehensive consumer and business education and law enforcement initiative targeting deceptive and misleading Internet promotion of products and services as cures or treatments for serious diseases. Just this summer, the FTC filed eight cases as part of Operation Cure.All, targeting companies that market a variety of devices, herbal products, and other di-

---

[7] *See* Federal Food, Drug, and Cosmetics Act, 21 U.S.C. § 301 *et seq.* The Hatch-Waxman amendments were contained in the Drug Price Competition and Patent Restoration Act of 1984, Pub. L. No. 98-417, 98 Stat. 1585 (codified at 15 U.S.C. §§ 68b, 68c, 70b; 21 U.S.C. §§ 301 note, 355, 360cc; 28 U.S.C. § 2201; 35 U.S.C. §§ 156, 271, 282 (1984)).

[8] *Abbott Laboratories,* No. C-3945 (May 22, 2000), and *Geneva Pharmaceuticals, Inc.,* No. C-3946 (May 22, 2000) (consent orders).

[9] *See also Hoechst Marion Roussel, Inc.,* No. C-9293 (May 8, 2000) (consent order). The Commission has also issued a complaint against *Schering-Plough* and two producers of generic drugs challenging their settlement agreements resolving patent litigation involving the drug K-Dur. Schering-Plough, No. 9297 (complaint issued April 2, 2001). Because the case is currently in administrative litigation, we cannot comment further.

[10] Combating health fraud has been a longstanding priority of the Commission. Since 1998, the Commission has brought 80 cases involving health and safety claims in advertising.

etary supplements to treat or cure cancer, arthritis, Alzheimer's, diabetes, and many other diseases.[11]

Although aggressive law enforcement is crucial, education may be the best consumer protection by preventing deception in the first place. As part of a comprehensive consumer education program, we recently partnered with the FDA to announce a new publication, *Miracle Health Claims: Add a Dose of Skepticism,* which provides detailed information on spotting and avoiding health care fraud. Another brochure, *Who Cares: Sources of Information About Health Care Products and Services,* published jointly with the National Association of Attorneys General, informs consumers about information for arthritis cures, alternative medicine, and other health issues, and where to file complaints about health care fraud. To alert older audiences about health fraud issues, the FTC works with other federal agencies, such as the Department of Health and Human Services' Administration on Aging, and with private groups, such as the AARP.

We will continue to use the Internet and other media to distribute our consumer education messages. Our Web site, www.ftc.gov, provides links to reliable health information, including www.healthfinder.gov, developed by the Department of Health and Human Services. In a little over one year, the FTC's Web-based consumer education material dealing with health issues has received nearly 80,000 hits.

To educate the unwary, the FTC also maintains three "teaser" Web sites—"Arthriticure," "Virility Plus," and "Nordicalite"—accessed using common search engines and designed to mimic fraudulent health care sites. When consumers attempt to order the bogus products, however, they are warned that if the promotions had been real, they would have been scammed. Most important, the site provides consumers with tips on how to identify Web sites that are most likely scams and directs them to sources of reliable information. In the last two years, the three teaser sites have received over 20,000 hits.

One specific type of health-related product—dietary supplements—will continue to receive special attention.[12] False or deceptive claims in the advertising for these products are especially rampant. Because total sales from such products were $15 billion in 1999 and are increasing annually by about 10 percent,[13] targeting deceptive claims for dietary supplements is an important use of FTC resources.

PRIVACY

Many consumers are deeply concerned about the privacy of their personal information, both online and offline. Although privacy 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 dumpster as by the one who steals that information from a Web site. Of course, the nature of Internet technology may raise its own special set of issues.

A majority of the Commission does not support online privacy legislation at this time,[14] but there is no doubt that consumer privacy is an issue that will continue to be studied and debated both at the FTC and in Congress. The Committee on En-

---

[11] *See Panda Herbal Int'l, Inc.,* No. C-4018 (Aug. 8, 2001) (consent order) (St. John's Wort and Herb Veil 8 marketed as treatment for HIV/AIDS and skin cancer, respectively); *ForMor, Inc.,* No. C-4021 (Aug. 8, 2001) (consent order) (St. John's Wort marketed as treatment for HIV/AIDS; colloidal silver and shark cartilage marketed as treatments for cancer, arthritis, and other diseases); *MaxCell Bioscience, Inc.,* No. C-4017 (Aug. 8, 2001) (consent order) (multi-ingredient product containing DHEA marketed to reverse aging and prevent age-related diseases); *Michael Forrest d/b/a Jaguar Enterprises of Santa Ana,* No. C-4020 (Aug. 8, 2001) (consent order) (miracle herbs and black box, magnetic pulser, and Beck-Rife units marketed as treatments for cancer and arthritis); *Robert C. Spencer d/b/a Aaron Company,* No. C-4019 (Aug. 8, 2001) (consent order) (colloidal silver marketed as treatment for cancer and many other diseases); *FTC v. Western Dietary Products Co. (Skookum),* No. C01-0818R (W.D. Wash., filed June 6, 2001) (herbal cure packages and "zappers" marketed as treatments for cancer); *FTC v. Western Botanicals, Inc.,* No. S-01-1332 DFL GGH (E.D. Cal., July 25, 2001) (Stipulated Permanent Injunction) (comfrey products); *FTC v. Christopher Enterprises, Inc.,* 2:01CV-0505 ST (C.D. Utah, stipulated preliminary injunction entered July 6, 2001) (comfrey products).

[12] In 2001, the Commission has brought 14 cases challenging advertising claims made for dietary supplements. During the period from 1998 through 2000, the Commission brought 46 such cases.

[13] Nutrition Business Journal, Volume IV, No.6 "Industry Overview 1999" at 3.

[14] Commissioners Anthony and Thompson continue to support legislation as recommended by the Commission last year. *See* Statement of Commissioner Sheila Anthony on the Commission's Privacy Agenda (Oct. 4, 2001); Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (May 2000) (Commissioner Orson Swindle, Dissenting, and Commissioner Thomas B. Leary, Concurring in Part and Dissenting in Part).

ergy and Commerce, and particularly the Subcommittee on Commerce, Trade, and Consumer Protection, have made significant contributions to the discussion of these issues. The Commission looks forward to continuing to work with the Committee and Subcommittee on these issues.

The FTC currently enforces a number of laws that address consumers' privacy.[15] The Commission intends to increase substantially the resources dedicated to privacy protection. Our initiatives in this area attempt to reduce the serious consequences that can result from the misuse of personal information and fall into three major categories: vigorous enforcement of existing laws, additional rulemaking, and continued consumer and business education.[16]

Law enforcement. The FTC intends to increase its law enforcement efforts in the following areas:

- Challenging "pretexting," the practice of fraudulently obtaining personal financial information, often by calling banks under the pretense of being a customer.[17]
- Enforcing privacy promises, focusing on cases involving sensitive information, transfers of information as part of a bankruptcy proceeding, and the failure of companies to meet commitments made under the Safe Harbor Program to comply with the European Commission's Directive on Data Protection.[18]
- Enforcing the Children's Online Privacy Protection Act, which prohibits the collection of personally identifiable information from young children without their parents' consent.[19]
- Enforcing the privacy protections of the Fair Credit Reporting Act, which ensures the integrity and accuracy of consumer credit reports and limits the disclosure of such information to entities that have "permissible purposes" to use the information.[20]
- Bringing actions against fraudulent or deceptive spammers.[21] Since 1998, the FTC has maintained a special electronic mailbox, uce@ftc.gov, to which Internet customers can forward spam. This database currently receives 10,000 new pieces of spam every day. We will use this mailbox to identify targets for law enforcement action.

Rulemaking. The Commission plans to engage in the following rulemaking activities:

---

[15] *See, e.g.,* Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.* (prohibiting deceptive or unfair acts or practices, including violations of stated privacy policies); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (addressing the accuracy, dissemination, and integrity of consumer reports); Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 *et seq.* (including the Telemarketing Sales Rule, 16 C.F.R. Part 310) (prohibiting telemarketers from calling at odd hours, engaging in harassing patterns of calls, and failing to disclose the identity of the seller and purpose of the call); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.* (prohibiting the collection of personally identifiable information from young children without their parents' consent); Identify Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (directing the FTC to collect identity theft complaints, refer them to the appropriate credit bureaus and law enforcement agencies, and provide victim assistance); Gramm-Leach-Bliley Act, 15 U.S.C. § 6081 *et seq.* (requiring financial institutions to provide notices to consumers and allowing consumers (with some exceptions) to choose whether their financial institutions may share their information with third parties).

[16] *See* Remarks of Chairman Timothy J. Muris, "Protecting Consumers' Privacy: 2002 and Beyond," The Privacy 2001 Conference, Cleveland, Ohio (Oct. 4, 2001).

[17] Some examples of recent "pretexting" cases brought by the Commission include: *FTC v. Information Search, Inc. and David Kacala,* No. AMD-01-1121 (D. Md. preliminary injunction entered May 4, 2001); *FTC v. Victor L. Guzzetta d/b/a Smart Data Systems,* No. CV-01-2335 (E.D.N.Y. preliminary injunction entered Apr.19, 2001); *FTC v. Paula L. Garrett d/b/a Discreet Data Systems,* No. H 01-1255 (S.D. Tex. preliminary injunction entered May 1, 2001).

[18] The European Commission's Directive on Data Protection became effective in October 1998, and prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. To bridge different privacy approaches between the U.S. and the EU, and to provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor" framework, which was approved by the EU in July 2000. Companies that self-certify to the Department of Commerce that they comply with the Safe Harbor Principles may be deemed by the EU to provide "adequate" privacy protection under the EU Directive. The FTC will give priority to referrals of non-compliance with safe harbor principles from EU Member States. *See* Department of Commerce's Safe Harbor Website, www.export.gov/safeharbor.

[19] *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq.* The Commission has brought several actions to enforce COPPA and its implementing Rule. *See, e.g. United States v. Lisa Frank, Inc.,* No. 01-1516-A (E.D. Va. filed Oct. 1, 2001) ($30,000 civil penalty).

[20] *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*

[21] Deceptive spamming is a prime example of high-tech fraud, discussed earlier.

- Considering whether to propose an amendment to the Telemarketing Sales Rule[22] to create a national do-not-call list to allow consumers to make one call to remove their names from telemarketing lists.
- Considering whether to propose an amendment to the Telemarketing Sales Rule to address the misuse of "pre-acquired account information," lists of names and credit card account numbers of potential customers. Misuses include billing consumers who believed they were simply accepting a free trial, or billing consumers for products or services that they did not purchase.[23]
- Completing the current rulemaking on safeguarding consumers' financial information pursuant to the Gramm-Leach-Bliley Act.[24]

Consumer and business education and outreach. The agency will continue to conduct workshops and other educational activities:

- Training law enforcement officials of a number of agencies to use the ID Theft database assembled by the FTC to spot trends that will help them prosecute those who engage in ID theft.[25]
- Promoting the FTC's toll-free number, 1-877-FTC-HELP, so that consumers know where to report privacy-related complaints.
- Hosting an interagency workshop on privacy notices required under Gramm-Leach- Bliley[26] to assess the impact of the notices, identify successful privacy notices, discuss strategies for communication of complex information, and encourage industry "best practices" and consumer and business education.
- Continuing to explore and monitor the privacy implications of new and emerging technologies through workshops, reports, and other public meetings.
- Joining with several companies and privacy organizations to develop a universal fraud complaint form that victims of identity theft can submit to each creditor involved. This form will help victims recoup their losses and restore their legitimate credit records more quickly.

ENERGY

As are health care and privacy, energy is of critical concern to consumers. The energy sector accounts for a significant portion of the nation's total economic output, and is a vital input to virtually all sectors of the economy. The FTC has long experience with energy issues. We have investigated a number of oil mergers in recent years and have brought cases where appropriate. For example, in *Exxon/Mobil*,[27] *BP/ARCO*,[28] and *Chevron/Texaco,*[29] the FTC required large divestitures of oil fields, refineries, pipelines, and gas stations to ensure that the combined companies would not gain market power at any level in the petroleum industry. We will continue to investigate thoroughly any activities that may raise competition issues.

The Commission recently announced a series of comprehensive conferences and hearings on "Factors that Affect the Price of Refined Petroleum Products" to further explore the practices of, and the changes occurring among, firms in the industry. The first conference was held on August 2, 2001, and agency staff is planning a sec-

---

[22] *See* Telemarketing Sales Rule, 16 C.F.R. Part 310.

[23] Recently, the Commission approved a federal district court settlement against Ira Smolev, Triad Discount Buying Services, Inc., and other defendants to resolve charges that they deceptively telemarketed buying clubs using negative option free trial offers and pre-acquired account information. The proposed order prohibits the defendants from obtaining account information from third parties, unless the third parties disclose to account-holders that they will transfer the account information and the account-holders agree to the transfer. The order also prohibits the defendants from transferring credit card information and personal identifiers to others, except as needed to process consumer-authorized transactions. *See In re Premier Membership Services LLC,* Case No. 00-35053-BKC-SHF (Bankr. S.D. Fla.).

[24] The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801(b) and 6805(b), requires the FTC to issue a rule establishing appropriate standards for safeguards to ensure the security, confidentiality and integrity of customer records and information.

[25] *See* Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028. This Act makes the FTC a central clearinghouse for identity theft complaints. Under the Act, the FTC is required to log and acknowledge such complaints, provide victims with relevant information, and refer their complaints to appropriate entities (*e.g.,* the major consumer reporting agencies and other law enforcement agencies).

[26] The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.,* requires financial institutions to provide notices to consumers and (with certain exceptions) allows consumers to choose whether their financial institutions may share their information with third parties. The FTC will undertake enforcement efforts to ensure that financial institutions comply with the law and will work to increase consumer awareness of the notices.

[27] *Exxon Corp. and Mobil Corp.,* No. C-3907 (January 26, 2001) (consent order).

[28] *BP Amoco p.l.c. and Atlantic Richfield Co.,* No. C-3938 (Aug. 29, 2000) (consent order).

[29] *Chevron Corporation/Texaco,* No. C-4023 (consent agreement accepted for public comment Sept. 7, 2001).

ond set of hearings. We expect that a significant number of experts in this field will participate at these hearings, which will be held early next year.

The FTC will investigate pricing behavior, where appropriate, in energy markets. In just the past year, we investigated various price spikes or pricing anomalies in petroleum products. Thus far, we have found no evidence of collusive activity in violation of the antitrust laws. Staff also investigated the recent gasoline price spikes in the aftermath of the September 11th terrorist attacks. Although these investigations did not find antitrust violations, Commission investigations nonetheless both have a deterrent effect on wrongdoing and provide the basis for action when anticompetitive practices have occurred.

Drawing upon our experience with energy and environmental matters, we have been advising states on emerging consumer issues as they deregulate and restructure their electricity and natural gas markets. A recent staff report prepared at the request of this Committee examines state retail electric programs to determine which reforms appear to have worked best in introducing competitive forces into the retail sale of electricity. The report concludes that, although the transition to competition is incomplete, the properly designed restructuring of this industry on the state level ultimately will result in benefits to consumers.[30]

The agency also focuses on energy issues that have a direct bearing on consumers' wallets. We have brought law enforcement actions challenging deceptive energy savings claims for various products.[31] We also educate consumers on energy issues by issuing alerts and other materials on topics such as saving at the gas pump, purported gas-saving products, and seasonal home heating and cooling tips. For example, the June 2001 consumer alert with gas-saving tips, *How to Be Penny Wise, Not Pump Fuelish,* has been well-received. We will update our Web site with a special "Energy and the Environment" page for easy reference of the relevant FTC rules, reports, and consumer and business education materials.

MERGERS

The FTC's careful evaluation of mergers will continue.[32] Although there has been much speculation about how the new Commission will regard merger cases, this area is yet another in which continuity, not change, will be the norm.[33] The agency will continue to follow the Merger Guidelines when assessing the impact of a proposed merger on competition.[34] Merger cases are fact intensive—the impact of a merger on competition can be assessed only with a careful investigation of the market or markets involved. If our investigation convinces us that a proposed merger will harm competition, the agency will assess proposed restructuring options presented by the parties to determine whether they will prevent that harm, or, when necessary, we will go to court to stop it.

Recent amendments to the Hart-Scott-Rodino Act[35] have reduced the overall number of HSR merger filings that the FTC and the Antitrust Division of the Department of Justice receive. Despite this reduction in HSR filings, the number of mergers raising competitive concerns appears to remain significant, and many are likely to present complex competitive issues that require thorough investigation. In

---

[30] Staff Report, Competition and Consumer Protection Perspectives on Electric Power Regulatory Reform: Focus on Retail Competition. This report was prepared in response to a request from Chairman Tauzin of the House Committee on Energy and Commerce, and Chairman Barton of that Committee's Subcommittee on Energy and Air Quality.

[31] *See., e.g., FTC v. Oil-Chem Research Corp. & Speedway Motorsports, Inc.,* No. 1:01 CV 00126 (M.D.N.C. filed Jan. 31, 2001) (challenging representations that vehicles using the zMax "Power System" will experience at least a 10 percent gas mileage improvement and reduced engine wear); *United States v. Intermatic Inc.,* No. 00C50178 (N.D. Ill. May 31, 2000) (consent decree) ($250,000 civil penalty in settlement of allegations that the company violated a 1979 FTC order by making unsubstantiated energy savings claims about an electric water heater timer); *Dura Lube Corp.,* No. 9292 (May 3, 2000) (consent order) (resolving allegations that respondents deceptively represented that their engine treatment product reduces emissions and improves gas mileage by up to 35 percent; order prohibits future deceptive claims and requires payment of $2 million in consumer redress).

[32] In the last five fiscal years, the FTC has reviewed over 17,000 HSR filings, opened 1,078 merger investigations, issued 190 second requests, and required modification to, or otherwise challenged, 147 mergers and acquisitions.

[33] *See* Remarks of Chairman Timothy J. Muris, "Antitrust Enforcement at the Federal Trade Commission: In a Word—Continuity," before the ABA Antitrust Section Annual Meeting, Chicago, Illinois (Aug. 7, 2001).

[34] U.S. Department of Justice and Federal Trade Commission, Horizontal Merger Guidelines (1992, revised 1997), reprinted in 4 Trade Reg. Rep. (CCH) ¶¶ 13,104 (1997), available at <http://www.ftc.gov/bc/docs/horizmer.htm>

[35] 15 U.S.C. § 18a, as amended, Pub. L. No 106-553; 114 Stat. 2762 (Dec. 21, 2000), effective February 1, 2001.

addition, the FTC will not limit its attention only to those mergers that are the subject of an HSR filing. In a complaint filed this month, the FTC alleged that an acquisition harmed consumers, even though it was not reportable to the antitrust agencies under the HSR Act.[36] It suffices to say that the merger staff likely will remain quite busy.

The FTC also continues to focus attention on reducing the burden of merger investigations. We are reviewing the burden caused—to both the government and the parties—by document productions received in response to so-called "Second Requests." We are also assessing whether merger investigations can be streamlined and shortened. As with all matters involving merger standards and procedures, we are working with the Department of Justice to address these issues. In particular, we are working with our counterparts at the Antitrust Division to determine the "best practices" that will minimize burdens while maintaining or enhancing our enforcement capability.

CONCLUSION

The agency's mission is to protect the welfare of consumers. Today's Federal Trade Commission has forged a widespread consensus on how to protect consumers and how to work with other federal and state agencies to provide maximum benefits for consumers from our limited resources. We will continue to use the full panoply of our institutional tools in fulfilling this important mission.

Mr. STEARNS. I thank the Chairman. I think the first question obviously is what would you say your top 3 to 5 goals that you will accomplish so that when you come back at the end of the 107th Congress, and hopefully the 1st of October, September of next year, that we can say that the Chairman said that his top 3 to 5 goals are X, and this is what he accomplished. And so maybe I will just start off with that question.

Mr. MURIS. Thank you, Mr. Chairman. I would——

Mr. STEARNS. I would just point out that we do have a vote here, and we have a series of a couple of votes. So I will try and get through my opening questions, and then we will recess and come back, and I know that the members will be asking questions thereafter.

Mr. MURIS. Thank you. I want to emphasize that we are standing on the shoulders of people who did an excellent job at the FTC, and we are hoping to build on the work that they did to do it even better.

On the consumer protection side, as I have mentioned, we are substantially increasing our resources on privacy. One of our issues that Mr. Markey raised is we are going to propose a National Do Not Call List, which for the first time will give consumers a one-stop place to call and have their names taken off of telemarketing lists. The Telemarketing Rule gives us that authority, and we have discussed it with the FCC, and I believe that will be a very important consumer initiative. Thus, implementation of our privacy agenda would be one point.

A second point on the consumer protection side would be to increase our effort against fraud, particularly on-line, although obviously we will look at off-line fraud as well. The diet supplement area is one of increasing importance, and we are looking there. Also, we are trying to use more sophisticated tools to search our data base, to look for patterns of illegal activity, and to try to detect and stop fraud even faster.

[36] *MSC.Software Corp.,* No. 9299 (complaint filed Oct. 10, 2001). The complaint filed this month challenges two acquisitions made by a dominant supplier of a popular type of advanced computer-aided engineering software. The complaint alleges that the defendant acquired its only two competitors in transactions that fell below HSR notification thresholds.

On the anti-trust side, with the slight receding of the merger wave, we are turning more attention to non-merger cases. We hope in the drug and other areas to have a very aggressive agenda to protect and benefit consumers. In the merger area, I would last point out that we are continuing aggressive enforcement. At the same time, we believe there are steps that we can take to reduce the compliance burdens of businesses that have grown quite large. Thus, these four areas are ones in which I hope we can accomplish a lot.

Mr. STEARNS. Let me just get to a question that a lot of people have asked me. Some have suggested that different types of fraudulent schemes have been used to fund terrorist networks in the United States. Do you have any evidence to support that contention?

Mr. MURIS. No. We are aggressively looking at scams that attempt to take advantage of the events of September 11, but we certainly have no evidence of the sort that you are suggesting.

Mr. STEARNS. Are you receiving any complaints?

Mr. MURIS. We are receiving many complaints about potentially fraudulent scams, but we have no evidence that links any of them to terrorist organizations. What we see are people trying to take advantage of the situation. For example, there are diet supplements that claim to cure or prevent anthrax, and people selling perhaps deceptive kits to test for various sorts of problems that are related to September 11.

Mr. STEARNS. And in the area of charitable giving are there any fraudulent schemes being perpetrated dealing with charitable contributions as of September 11?

Mr. MURIS. There are dozens of law enforcement agencies that we are working with that are searching for such schemes. At the moment, although there have been a few problems that would surface briefly and then the companies would desist, there do not appear to be problems. Again, there are dozens of law enforcement agencies looking at this issue, including us.

Mr. STEARNS. Recently, we have begun to see reduced risk tobacco product ads claiming that those products pose a lower health risk than regular tobacco products. Does the Commission have the requisite authority to review the efficacy of these ads, and if so, will it?

Mr. MURIS. Yes on both accounts. The Commission has a long history in the tobacco area. Although many of the issues of tobacco advertising were resolved in the agreement between the tobacco industry and the States, this is an active issue. I would certainly recommend that the Commission move appropriately against any deception or unfairness in such advertising.

Mr. STEARNS. Just briefly. Is there anything as a result of September 11 that you are facing that part of the emergency funding and supplemental that you see an area where you need beefed up support that we in Congress should give you?

Mr. MURIS. In terms of resources, the Commission in the budget that is about to pass will receive a modest increase. I personally think another modest increase would be beneficial. Because of September 11, we have diverted resources from some other areas that

are important, and I do think that modest increases in our budget are appropriate.

Mr. STEARNS. Okay. Mr. Chairman, we are going to take a recess for two votes, and it will probably be about 20 minutes, and we appreciate your indulgence. You have been up here many times and so you understand this.

Mr. MURIS. Yes, thank you.

Mr. STEARNS. And the subcommittee will take a recess.

[Brief recess.]

Mr. STEARNS. The subcommittee will come to order, and I have finished with my questions, and I will go now to the ranking member, Mr. Towns of New York.

Mr. TOWNS. Thank you very much, Mr. Chairman. Talking about identity theft, is there any one document or one piece of personal information that seems to be used more than others by those that engage in identity theft?

Mr. MURIS. Well, certainly the Social Security number is. If you want to steal someone's identity that is an excellent way to do it. There are people who just get credit card numbers, and that can be a problem as well, in the sense that if you get the credit card number, then you can certainly run up bills.

Mr. TOWNS. Since September 11, there have been numerous press reports about how easy it is in certain States to get a drivers license. One State has reportedly issued more than a hundred-thousand licenses all with the number 99999 as a substitute for a Social Security number that could not be provided.

Do license requirements for a drivers license at that level pose a significant problem in controlling identity theft, and if so, what should be done about it?

Mr. MURIS. That is certainly a good question. Congress had us create an identity theft lab, and we have about 130,000 complaints and inquiries. I have actually sat in that lab and listened to calls. My experience, and I am new at this particular issue, is that the driver's license is less of a problem than the other problems that I have mentioned, but I would be certainly glad to look into it.

Mr. TOWNS. All right. How many of these identity theft complaints received by the FTC would you say constitute actual violations of the law, and how many result from legal commercial practices?

Mr. MURIS. Certainly most of the complaints that we have received are identity theft. There are people who have charges on their bills that they did not make. There are serious problems in so-called pretexting which Congress gave us authority to act against, and which we are acting against. Pretexting is when someone calls a financial institution and pretends to be you, and gets information. The Commission brought some recent cases, and I think that is an outrageous practice. We have complaints about it.

Mr. TOWNS. Thank you. Let me say that the means with which web sites collect and distribute non-public personal information is by-and-large governed only by the industry self-regulation. We support the FTC's efforts to enforce industry promises.

However, what can be done to address web sites that choose not to participate in self-regulation, having inadequate or no privacy policies at all? What can we do?

Mr. MURIS. One of the things that is under-appreciated by some is the extent to which there has been considerable progress in posting privacy policies. All of the top web sites have such policies.

If the operator of a website permits payment using a VISA card, for example, VISA requires that the website post a privacy policy. Obviously, most web sites that do transactions would accept a VISA card.

Moeover, in the privacy area, in terms of security, when information is leaked or sold either intentionally or negligently, I think that under certain circumstances that can be a violation of the FTC Act, and we are moving in that area.

Mr. TOWNS. One final question, Mr. Chairman. In many communities across the country predatory lenders swindle unsuspecting consumers out of millions of dollars every year. What can the FTC do, if anything, about that?

Mr. MURIS. The FTC has been quite aggressive under our predecessors in attacking predatory lending. There are some particularly bad practices out there, and the cases have been appropriate. We are prosecuting them vigorously, and we are looking for others.

Mr. TOWNS. Thank you very much, Mr. Chairman. I yield back.

Mr. STEARNS. I thank the gentleman. The chairman of the full committee is here, Mr. Tauzin, is recognized.

Chairman TAUZIN. Thank you, Mr. Chairman. Let me welcome you, Chairman Muris, and I know that our written statements have been made a part of the record, and in the written statement that I prepared for today's hearing I commended you.

And I wanted to commend you personally for the statements that you made in Cleveland, I think it was, regarding the privacy issue, and the fact that you intend to refocus the Commission's attention to enforcing law in these areas, and insisting that in fact that as much as possible that the private sector respect the principles of privacy that have been outlined by the Commission on previous occasions.

And also I wanted to thank you for attending the privacy conference that Chairman Stearns and the Chamber of Commerce held just recently at Landsdown, where in fact we got a better sense of what the outstanding legislative initiatives may look like next year when we take the issue up.

And particularly the concern that the States are beginning to move, and particularly California, toward adopting State privacy policies that might conflict with other States and Federal policies in interstate conference.

And I want to thank you again for participating in that session and for giving us the benefit of your thoughts and advice in regards to that. And in that regard, while you indicated initially in that speech that you thought that legislation might not be as necessary as good enforcement, you seem to have conceded the notion to us at that hearing that we have sort of been wrestling with as well that if we are going to have a privacy policy that works for the country, that having States and/or different agencies adopting conflicting policies could cause us great harm.

And that perhaps that we need at least some sort of standard, some basic principles of policy upon which all of us can function in interstate commerce. Is that correct?

Mr. MURIS. Yes, Mr. Chairman. I appreciate your comments. I have enjoyed working with you so far, and look forward to working together in the future. The point that I made in that speech, and also at Landsdowne, was that the particular issue of broad based, Internet only legislation is still premature at this moment. I did say and I do believe that the best argument for such legislation is if we start getting inconsistent State laws. At the moment that has not happened, but I understand that there is some danger that that will occur.

Chairman TAUZIN. Well, California came within the half-foot line in football analogy from getting it done, right?

Mr. MURIS. It was financial institutions. It was not the on-line privacy issue, but in that financial institution area it would create a serious problem.

Chairman TAUZIN. And we also talked about the concept of creating a safe harbor for private institutions that work within self-regulatory regimes, and sealed organizations, so that they might not be affected by any kind of Federal statutes or rulemaking.

And at the same time, some sort of provision to catch those that refuse or are unwilling to work within self-regulatory structures. Is that a good frame upon which we should proceed?

Mr. MURIS. Certainly if you are going to do legislation, legislation that gives clear guidance with things like safe harbors would be appropriate. Quite frankly there is a lot that we can do under the FTC Act, and I thank you for you commending us for doing more. One of the things that we are doing both in our cases and in working with the self-regulatory agencies is trying to set out some clear guidance. But again if you are to do legislation, that would be appropriate.

Chairman TAUZIN. And I want to touch on a topic that is going to get I think a lot of attention next year. We are going to begin work on a reauthorization of the FDAUFA statutes. FDAUFA is a statute that deals with the FDA, and has to do with the user fees that are collected for studying and for approving new drugs.

When that statute opens, it is very likely that we are going to get back into tobacco, and so I want to ask you a couple of tobacco questions. We are beginning to see advertisements by tobacco companies regarding their efforts to reduce the carcinogenic compounds that are found in tobacco, and their efforts to market products that have less of those carcinogens in the tobacco.

We are also beginning to see new products, new smokeless tobacco products, and we will begin to see advertisements on those products. What is the FTC's role when it comes to advertisements or claims about safer, or different, forms of tobacco products?

Mr. MURIS. The FTC has an important role involving advertising. As I have stated, this is an area in which we should be aggressive in policing advertising for deception and unfairness, and I believe that the FTC will continue to do that.

Chairman TAUZIN. So that if a tobacco company were making a claim that some tobacco product had a less serious deleterious health effect, and that it was safer in some respect, or that it contained less carcinogens, is it without the FTC's jurisdiction and authority to examine those claims and to enforce the law against

false, misleading, or deceptive health claims in regard to these tobacco products?

Mr. MURIS. Absolutely. We have that authority now, and I believe the FTC would exercise it appropriately.

Chairman TAUZIN. I thank you very much, and I yield back, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. The gentlelady from California, Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Chairman, and welcome, Mr. Chairman.

Mr. MURIS. Thank you.

Ms. ESHOO. It is good to see you, and have you here. I wrote to you last month with some of my concerns, and so I am looking forward to hearing back from you on the specifics of that letter.

But let me ask some broader questions of you this morning. I want to commend you for proposing that the FTC's enforcement of existing laws—that your budget be, and your staff be increased by I think 50 percent.

I think that is what you were asking for, and to devote it to consumer privacy issues. Where is that right now? I mean, very quickly. Is it in an appropriation bill?

Mr. MURIS. No, what I was saying is that we would increase within our total budget our resources——

Ms. ESHOO. And how much is that?

Mr. MURIS. In the fiscal year that just ended, we spent about 35 people full-time.

Ms. ESHOO. And how much is that? So you are going 50 percent over that?

Mr. MURIS. Yes, 50 percent over that. Actually, it is a little more than 50 percent, but we will spend somewhere in the range of 55 to 60 people working on privacy, which is a slightly more than 50 percent increase from the last year. I am talking fiscal years, and the fiscal year that just began last month.

Ms. ESHOO. Yes. I am aware of that. Thank you. Now, in the 50 percent increase of that staff, what exactly will they be doing relative to consumer privacy issues? Can you give us a thumbnail sketch?

And I think you know where I am going. Since it has been your recommendation to kind of pull up the emergency brake so to speak on legislative action, what I am pursuing is exactly how you are going to make use of the staff at the FTC on this.

So how are you instructing them, and what exactly will they be doing, and how do you pursue bad actors? What is a bad actor, and how do you come down on them?

Mr. MURIS. We have five very recent privacy statutes that we enforce and we are increasing our enforcement. We have statutes dealing with financial privacy, children's privacy, health privacy, and we have recent amendments to the Fair Credit Reporting Act. We also have recent identity theft statutes. Plus, we have our own statute that we use in privacy, and we are increasing our resources by 50 percent to enforce those statutes. We will follow a tripartite strategy of case enforcement, and that particularly deals with the——

Ms. ESHOO. How aggressive has this been, or is it something that is awakening and really being shaped by you?

Mr. MURIS. Privacy is a relatively new issue for the Federal Trade Commission, but in the last few years the Commission has become a leader in the privacy efforts. I thought particularly with these new statutes that a further increase in our effort would be appropriate. We are going to bring cases. We also have excellent relations, and——

Ms. ESHOO. How do you determine bad actors? What is the process for the Commission and its staff to pursue this? Again, I think it is obvious why I am asking these questions. What I am concerned about, and I know that obviously the letter that I sent to you states this, that I think in some areas we need umbrellas, Federal umbrellas, because of the 50 States, and the patchwork quilt.

It is very difficult I think to give the answer to our constituents of where we are on privacy, and how we have made progress as a Nation, and what is acceptable, and what isn't acceptable, and how we pursue, and what the rules of the road are.

Right now if I were to describe it, I think it is like nailing jello to a wall. I don't really think we have anything. I think we have some operating principles that people think are good things to go by. I certainly have introduced legislation on this, and others have.

But what I am trying to nail down are some of the bright lines of the FTC. So how do you determine bad actors? What are you going to do about them? How does the staff bring this about? Are they reported, or do you do this internally?

And I note that in your comments that you said that about a hundred of the top companies have posted. Well, there may be a hundred top companies, but I can think of at least 50 brand-named companies in my Congressional District. And so a hundred is not that many out of our country I don't think. So, anyway, go at it.

Mr. MURIS. Sure. First of all, I apologize. I am unaware of your letter. Unfortunately for 2 weeks we had no mail delivered to us, and if you sent it in the regular mail, it probably——

Ms. ESHOO. We will fax it to you. How is that?

Mr. MURIS. I appreciate it. It probably was rerouted to Ohio, and we are now starting to get mail delivered. We have a complaint system, and it is one of the ways that we look for cases.

Ms. ESHOO. So, from the outside coming in?

Mr. MURIS. Yes, which we are improving. That complaint system had never specifically addressed privacy concerns before. The privacy groups asked to change our complaint system to track privacy complaints. I thought that was an excellent idea, and we are doing that.

Under the specific statutes that we enforce, we look for people who create problems. For example, the Fair Credit Reporting Act was our first privacy statute. It is 30 years old, and it is an important privacy statute.

One of the things that it says is that if a consumer is denied credit, insurance, or employment, because of something that is in his or her credit report, the consumer has to be told that that was why. And if the consumer is told, as credit reports aren't always perfect, then they know that there is a problem and to check on the problem.

We are stepping up and increasing our enforcement of that provision. We are also quite frankly under the——

Ms. ESHOO. So if someone violates that and you find them, quote, guilty, what happens to them?

Mr. MURIS. We have a variety of remedies that we can seek. In some cases, depending on the violation, we can get monetary relief. Under the Fair Credit Reporting Act, for the most part, we do what is called a cease and desist order.

Ms. ESHOO. Let me ask you this, because I think the clock is going to go off, or maybe the red light is already on.

Mr. MURIS. Okay.

Ms. ESHOO. In the areas that you listed out, and where you have jurisdiction, in the last year how many violations that were either detected or reported from the outside to the FTC have been adjudicated and fines levied, or whatever the process is?

Mr. MURIS. Well, we have brought numerous cases. Under the Children's Privacy Act, for example——

Ms. ESHOO. No, all of them combined.

Mr. MURIS. All of them combined? I am not sure what the answer is.

Ms. ESHOO. Do you think it is aggressive?

Mr. MURIS. One of the reasons that I proposed a 50 percent increase in resources is that I thought that we could do better. The Commission has done a good job in the past in making privacy a central issue, but I proposed an increase because I thought it was an important issue that deserved more effort.

Mr. STEARNS. The gentlelady's time has expired.

Ms. ESHOO. May I ask unanimous consent for one more question?

Mr. STEARNS. So ordered.

Ms. ESHOO. Thank you, Mr. Chairman. Why do you consider the Internet and main street, and how they operate, one and the same? Why do you treat them the same way?

Mr. MURIS. The point that I made about on-line and off-line, which I know that Chairman Stearns' proposal agreed with, is that collecting information is increasingly becoming seamless. Companies that collect information off-line and on-line are integrating those systems. To have one set of rules for the Internet is going to punish the Internet relative to off-line. For the sensitive financial and health information, which are the most important kinds of collections, we ought not to punish on-line.

Ms. ESHOO. I am not so sure I understand your answer. If you draw a line between the two because they operate differently—Mr. and Mrs. Smith's store on main stream, versus an on-line privacy—I don't understand why you would treat them the same?

Mr. MURIS. The issue that we are talking about and that is relevant for us is the collection of sensitive personal information. If you have tougher standards for the——

Ms. ESHOO. But it operates differently though.

Mr. MURIS. If you have tougher standards for the collection of information on-line than you have for the collection of information off-line, then you are punishing the on-line companies.

Ms. ESHOO. And how would the FTC enforce that?

Mr. MURIS. How? Certainly the FTC will enforce whatever laws Congress tells us to enforce. But my point is that we ought not to

penalize the development of the Internet by adopting tougher privacy standards for the collection of information on-line than for the collection of information off-line.

Ms. ESHOO. And my final comment, and I thank the Chairman for his patience, is that I think that if you don't do more to build the confidence of the American people in transactions on-line, then we have lost the battle.

I think that there is enough out there that is cutting into this confidence. We have many, many overlays today since September 11, but I think that confidence is the gold standard when it comes to our markets, and I think confidence is the gold standard relative to the Internet.

I think that confidence, confidence, confidence, being built in each important sector just cannot be overlooked. So I think that we are missing that opportunity, but I look forward to working with you. Thank you, Mr. Chairman.

Mr. STEARNS. Thank you, gentlelady. Mr. Terry is recognized.

Mr. TERRY. Thank you, Mr. Chairman. We telephoned your office to discuss an issue in my home town with one of my constituents, and a couple of hundred of the employees that work for Paypal, in a kind of interesting issue regarding vertical integration of E-Commerce on the Internet, and who can control the payment methods when making purchases on the Internet.

So let me just ask you the general, and then if you can move to the specific, but generally what is the philosophy of your department, of the FTC, regarding anti-trust on E-Commerce and vertical integration.

And whether or not specifically then in electronic commerce if the method of on-line payment fits into that philosophy, and again whether or not the philosophy will change from past to now under your leadership.

Mr. MURIS. To start at the most general level, we enforce the anti-trust laws, and the anti-trust laws—mostly, but not exclusively—focus on agreements among competitors and on so-called monopolistic practices. It is possible in certain circumstances to bring a case based on vertical integration. The law is very tough because it is premised on lots of empirical evidence that vertical integration often benefits consumers.

Many of these cases frequently involve contractual disputes, contractual issues more than they involve anti-trust law. If you have a situation, however, when you have a company that really has substantial market power, that company can misuse vertical integration in a way that harms consumers. It is a tough case to bring and win.

Mr. TERRY. This issue is somewhere in the process at the FTC, and where is it in—well, you mentioned about whether somebody has sufficient market power to really cause damage. Has there been any determination or early thoughts that E-Bay in this particular situation has that level of market power to really wreck havoc on these small businesses that focus on electronic payment?

Mr. MURIS. We would take a look at situations involving abuses of market power. I personally do not know enough about the specific matter that you have referenced. I just found out about it last night, about the particular facts, and can not comment on those

facts. As I said, there can be appropriate cases, but they are relatively few and they are hard to win.

Mr. TERRY. Despite the difficulty in winning those, is this somewhere in the process of being reviewed at the FTC?

Mr. MURIS. Again, part of the problem is that we have had this mail problem like everyone else has, and we will certainly look at any recommendation we receive from you or any other members of the committee.

Mr. TERRY. I appreciate that. Thank you. I yield back.

Mr. STEARNS. The gentleman yields back the balance of his time. The gentleman from Massachusetts, Mr. Markey, is recognized.

Mr. MARKEY. Thank you, Mr. Chairman, very much. First, I would like to compliment you, Mr. Chairman, on announcing that the Commission is going—and I am reading from your testimony, that the Commission plans to engage in the following rulemaking activities to consider whether to propose an amendment to the telemarketing sales rule to create a national do not call list to allow consumers to make one call to remove their names from telemarketing lists.

What greater gift could you give to the American people than to just have one call where you say I don't want anybody else to call me again. You know, just keep them all away from my house.

So this has always been my dream when I authored the Act in 1991. That the day would arrive when out of the Federal Communications Commission, or the Federal Trade Commission, that they would do this, and it was always my intention.

Because you just get worn down. You keep telling different companies, and then you can't remember which company it was that you told 3 weeks ago that you didn't want to be called again, and so you are not sure whether you should be mad at this one person who is calling you, but you are just mad in general when you hang up because you were waiting for a call from your Aunt Margie, and these people are just interfering with it.

So I want to compliment you for doing it, but the hosannas will rain down on you, Mr. Chairman, if more than just considering whether to propose an amendment that you actually announce that you are going to propose an amendment.

You name will ring in the heavens of this institution and all across the country, because there never again will be a greater achievement that will attach to your name than if you actually do it. So I would just like you to know that on this issue that there are no Democrats, and there are no Republicans. We are united at water's edge here in our battle against telemarketers.

So you will hear no dissenting views on this, I think, except from companies that make money off of it. And the interesting thing about privacy policy generally as you know is that we have this privacy paradox, which is that if in fact a company posts a privacy policy, and then violates its own policy, then the Federal Trade Commission can bring an action against them for engaging in unfair and deceptive practices.

However, if the company never posts a privacy policy, but engages in personal information hijacking, then there is nothing that you can do about it, which is just totally backwards. The companies that don't protect privacy at all, you can't do anything about, and

the companies that say that they are going to protect privacy and then don't, you have an action against them because they didn't do as much as they promised that they were going to do.

So the question that obviously constantly arises is why don't we just put a regulation on the books so that these bad people who don't protect any privacy at all have real protections which are built in to the law so that there is a minimal level of electronic ethics that every company has to abide by, in terms of their relationship with the consumer.

Mr. MURIS. I certainly appreciate your comments on the telemarketing sales rule amendment, which we are about to propose. Obviously, we have to look at the rulemaking record in making our final determination.

The problem that I have at this time with on-line legislation, besides the fact that it would discriminate against on-line commerce, is that it is notice based. This spring and summer everyone in America received several notices from their financial institutions, as required by Gramm/Leach/Bliley. We need to understand how to do notice legislation better before we move to new notice-based legislation. We are holding a workshop on December 4, where we are bringing in everybody, the agencies who enforce Gramm/Leach/Bliley and the people who send out the notices. We will try to see how we can make it work better. Quite frankly that experience this spring and summer was not a very salutary experience for notice-based legislation.

Mr. MARKEY. Can I tell you, Mr. Chairman, that I am the author of that language as well, although it is included in the bill that you keep mentioning, those three names. But it is the Markey language that is in there.

And what we are trying to do with the financial services industry is to deal with the fact that there is an underlying pathology in the financial services industry which doesn't want to provide any privacy protections whatsoever, which is why they fought us on this committee, which is where it came out of, the privacy language.

They actually defeated it in the Senate and in the Banking Committee across the corridor from me. So they are kind of like—they are in a recovering privacy violators program. There is a deep-seeded pathology that they have.

And then when you say to them, now, please give notice to people that their privacy may or may not be protected, and here is your two-page document that you have to sign, and this or that, and there is triple-negatives that are in it that would require a $500 an hour lawyer in order to figure it out, of course it is not successful.

However, if you allowed a bunch of sixth graders to sit around and just draft it up, or just check it this way or that way, and it is going to cover you for everything, then it would be all done.

And so it is not that complicated in fact. In just requires somebody in your staff to just kind of draft it up, and just say here is what you are going to do from now on or else we are going to sue you, and it would be all solved for the next round that we would have to go through.

But it doesn't require a lot to figure out that the people who were charged with doing it at their company didn't want to do it. I have

one final question, Mr. Chairman, if I may, and I apologize, and ask for your indulgence.

In recent days there has been an announcement of media mergers that are going to receive a lot of attention. I think that one of the ways in which we can gain some insights as to what needs to be done would be looking just backwards a little bit toward the AOL-Time Warner merger so that we can assess the conditions that were imposed upon that merger, in terms of how successful they have been.

So I would just like to just ask this quick question, and then ask you to submit to the record, to the chairman, and to the full committee, or to the subcommittee, in writing your answer to this question within 2 weeks, and I would appreciate it.

The consent AOL-Time Warner order, as summarized by your agency's website, stipulates, quote, that AOL would be required to open its cable system to competitor ISPs, prohibited from interfering with content passed along the bandwidth, and contracted for by non-affiliated ISPs, and from interfering with the ability of non-affiliated providers of interactive t.v. services, to interact with interactive signals, triggers, or content that AOL-Time Warner has agreed to carry; and prevented from discriminating on the basis of affiliation in the transmission of content, or from entering into exclusive arrangements with other cable companies with respect to ISP services or interactive t.v. services.

And required to market and offer AOL's digital subscriber line services to subscribers in AOL's cable areas where affiliated cable broadband service is available in the same manner, and at the same retail pricing, as they do in these areas where affiliated cable broadband ISP service is not available.

So what I would like to ask, Mr. Chairman, is perhaps not 2 weeks, but perhaps by December 1, if the Agency could submit to us in writing how much compliance in their opinion they believe the AOL-Time Warner has given to this language.

Mr. STEARNS. I think that is a good question that we would like to have.

Mr. MARKEY. And if I may, we would like a status report on each condition so that we can have an idea in each area how well the FTC is overseeing the implementation of the Act. Thank you, Mr. Chairman.

Mr. STEARNS. Yes, I thank the gentleman.

Mr. MARKEY. Would the Chairman be willing to do that?

Mr. MURIS. Yes, sir.

Mr. STEARNS. Okay. The gentleman from New Hampshire, Mr. Bass, is recognized.

Mr. BASS. Thank you, Mr. Chairman. Mr. Chairman, the Oversight and Investigation Subcommittee had a hearing yesterday on the issue of charitable—the disposition of funds raised for charitable purposes in the aftermath of the September 11 tragedy.

And I asked Mr. Beamis yesterday about the issue of whether he thought the FTC needed additional authority to oversee the practices of charities, and I am just wondering what your thoughts are on that subject.

Mr. MURIS. One of the issues in the national do not call list is that it would cover 80 percent of the calls, but it would not cover

political fundraising calls, or most charitable calls. If Congress proposed to extend our ability to cover charities in that sense, that certainly would be something that we would consider. You recently amended the Telemarketing Sales Rule to give us more authority over charities, and we are trying to understand the new law.

Mr. BASS. In the Patriot Act you mean; is that right?

Mr. MURIS. Yes. When there is outright fraud, we already have sufficient jurisdiction. There are serious constitutional problems in dealing with charities, however. A final issue with non-profits in general, and not just charities, is that their exemption causes us a problem under the anti-trust laws. There can be anti-competitive conduct by non-profits that we cannot reach, although the Justice Department, which also enforces the anti-trust laws, can reach those.

Mr. BASS. Okay. Another issue is what level of success have you had with enforcing rules when the seller is overseas, and it is probably an Internet more than anything else issue.

Mr. MURIS. That is an excellent question and it is one to which we need to pay increasing attention. Cross-border fraud is a growing issue. As we have moved in the United States, for example on the telemarketing front to crack down on fraud, many telemarketers have gone to Canada. We have good cooperation with the Canadians, and we are hoping to increase it.

I hope to emulate something that occurred on the anti-trust side. Over the last 15 years, anti-trust authorities internationally have achieved good cooperation in attacking price fixing. I hope that we can emulate that cooperation on the cross-border front. We have begun with Canada, and I hope that we increase our work in that area.

Mr. BASS. Do you need Congressional help to achieve that, or can you do it anyway?

Mr. MURIS. We might need Congressional help, and it is something that I am studying. I certainly would not hesitate to ask for your help, and this committee would obviously be the place to start.

Mr. BASS. One last question. Mr. Tauzin talked about the issue of privacy and preemption of State regulatory efforts. Are there any other areas where you think the FTC may have some issues with State regulation versus Federal?

Mr. MURIS. For the most part, we have an excellent cooperative relationship with the States. In fraud in particular, we bring cases together with the States. The same thing happens on the anti-trust side. It is clear that State legislation can cause problems. In terms of enforcement, it is mostly cooperation and not any sort of adverse competition.

Mr. BASS. Thank you, Mr. Chairman.

Mr. STEARNS. Thank you. I thank the gentleman. Mr. Deal is recognized.

Mr. DEAL. Thank you, Mr. Chairman and thank you for being here today as well. I have a couple of very diverse areas, and to follow up on your last comment, I have just a matter of inquiry with regard to the enforcement of fraud schemes in cross-country relationships.

Is there anything in WTO that binds all of the WTO members to a common agreement with regard to prosecuting those, and if

not, is that an area that perhaps should be looked at as one that our country should push?

Mr. MURIS. No, there is not. We should push bilateral agreements. We are not at the stage yet when a multi-lateral WTO agreement would be appropriate, but certainly bilateral agreements, which is what we first used in the anti-trust laws, are appropriate. I plan to make this a priority.

Mr. DEAL. I would urge you to do that, and as we go forward with the bilateral agreements, certainly I think we ought to make it a priority in those agreements. Let me go—we all have our favorite issues that we have complaints about, and as a member who has three—my wife and my own family members, who are 86 through 95 years of age, and live with us in our home, I have become increasingly aware of the fraud that is attempted and continue to be perpetrated and aimed at senior citizens and the so-called sweepstakes type solicitations.

I assume that at least part of that issue is within your jurisdiction, and I would just ask you if you would bring us up to date as to what has been done. I mean, if I could just add together all of the winnings that these three senior members of our family have been told they have won, they would all be multi-millionaires.

However, if I added up the amount of fees that have to be paid just to get their earnings, whether it be send us $11.65 so that we can mail you your $25,000 check, and we will do so immediately, I think we have sort of all lost focus of that problem, and to me it is a huge problem.

There may be problems in the mail elsewhere, but there is no problem with those letters getting through. What is being done and what if anything else do we need to do legislatively?

Mr. MURIS. The situation that you described would probably be illegal. The Commission has brought cases. The typical one involves consumers paying money for a promise to help them win. The States were very active and have announced in the last few years settlements with major sweepstakes companies. Congress in the last year or 2 passed legislation requiring additional disclosures. Thus, there has been much that has happened on this front.

We in general work with the AARP and other groups on particular problems that the elderly have. Health care issues are probably a bigger issue, but sweepstakes is a significant issue as well. We have been aggressive in those areas.

Mr. DEAL. Do you need any other legislative authority to assist in that regard?

Mr. MURIS. This is an area where our legislative authority is quite good.

Mr. DEAL. All right. Let me move to a totally different subject, and that is the area of health care, and your written testimony I think is very good in that regard, in your efforts to deal with fraudulent and scam operations in the health care area.

Let me bring the question as it relates to an issue that we get complaints from in my office, and that is the question of the ordering of prescription drugs over the Internet. And the question that is raised by many local pharmacists, for example, that the adequate safeguards that are required of a local pharmacist, in terms of advising, and follow-up, and counseling, are not accompanying

those kinds of orders. Is that an area that you have been involved with, and what is the status of that? If you would comment.

Mr. MURIS. In general we have been looking at several issues of products migrating on-line—whether they are sold deceptively and whether there are restrictions imposed upon them that are appropriate. We have looked at some issues involving the on-line sale of pharmaceuticals. I would be glad to get back to you with the details, because I do not know specifically the status.

Mr. DEAL. All right. If you would, because I think as you recognized as more migrates to that medium for purchase, we can't tighten up on the local pharmacist, and at the same time relieve the other sales venues from those kind of controls.

And one final very unrelated question, and that is the safe harbor provisions that the EU has put in place. I noticed in your testimony, and I believe it is Footnote 18 to the testimony, that your organization is giving priority to complaints of non-compliance.

I think that all of us recognize that some people think that we are going too far in enforcing European law on American companies. What is your general view of the safe harbor under the EU and your role in enforcement?

Mr. MURIS. It is important to understand what my predecessor promised to do, which promise I will abide by. We are not going to enforce the European law. What we are going to enforce is American companies promises to their consumers.

In this case, if they promised that they will enforce certain privacy provisions and if they break that promise, we will act.

Mr. DEAL. That is a good distinction. Thank you very much, and thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Before we close, Mr. Chairman, you touched in one of your answers to one of my colleagues that as a result of September 11 and these charitable contribution funds, there have been some complaints that they have not distributed the money.

You sort of indicated that perhaps you could be given more authority to help out in this area. The State of Minnesota has a proposal that if you have a charitable, not-for-profit fund, that you have to notify the State.

And second that you have to provide information on your expenses and your overhead. You don't have to provide the privacy of the individuals contributed, but you have to show how much money was expended in overhead, or administrative expense, and how much was given out in a charitable way.

And I was wondering if you thought on a national basis that we should have perhaps as a start just for national emergencies, like Hurricane Andrews down in Florida, or September 11, and perhaps we have, god forbid, additional terrorist acts, that these national tragedies which we see people develop huge amounts of money, and yet the money is not distributed, is it possible that we should have some national legislation that would give you more power so that you would develop, say, a data base on these people to make sure that they are legitimate, and that there is no fraud.

And then second that they have a reporting system where they would have to tell what their expenses are and how much money they give out, because just the light of day, the sunlight, would per-

haps give the American citizens knowledge, whether they are giving money to the United Fund, or the Red Cross, or the Julianne Fund, what it is doing with the money and when. I would just be curious to hear your comments.

Mr. MURIS. That is an excellent question, Mr. Chairman. This is not an area in which we have current jurisdiction, and I would have to look at it more closely to give you a definitive answer. I do know that there are serious constitutional issues just in doing what you are stating, particularly with religious institutions. The Supreme Court struck down a State law that required some of the information that you are discussing on First Amendment grounds.

I certainly think that sunshine is appropriate. I know that there are some self-regulatory organizations that provide that information. Through our consumer education programs, we try to help educate consumers. But on the issue of additional legislation, I would have to study it more closely.

Mr. STEARNS. You might do that for me and just get back in writing.

Mr. MURIS. Yes.

Mr. STEARNS. And as I pointed out, as I understand it, some States have been successful in this, and have met the Constitutional requirements. So that is the area that we would work at. The ranking member, I will ask for his——

Mr. TOWNS. I have a unanimous consent request.

Mr. STEARNS. Yes.

Mr. TOWNS. I ask consent for all members to be able to submit statements for the record.

Mr. STEARNS. Without objection, so ordered.

Mr. TOWNS. And on that note, I ask that Congresswoman DeGette, I would like permission for her to submit for the record a report of the Business Roundtable, dated July 2001, entitled, Information Privacy, the Current Legal Regime.

Finally, Mr. Chairman, I request permission for Mrs. DeGette to submit questions to the Chairman, and that his responses be included in the record of this hearing.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. TOWNS. Thank you.

Mr. STEARNS. Mr. Chairman, thank you very much for your patience while we went to vote and we are delighted that we had this first opportunity to engage in a discussion, and we look forward to seeing you again. With that, the committee is adjourned.

Mr. MURIS. Thank you.

[Whereupon, at 11:58 a.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

FEDERAL TRADE COMMISSION
OFFICE OF THE DIRECTOR, CONGRESSIONAL RELATIONS
December 5, 2001

The Honorable CLIFF STEARNS
Chairman
Subcommittee on Commerce, Trade and Consumer Protection
Energy and Commerce Committee
United States House of Representatives
Washington, D.C. 20515

DEAR CHAIRMAN STEARNS: Enclosed please find the written responses from Chairman Muris to questions raised during the November 7, 2001 hearing. Please let me know if I can be of further assistance.

Sincerely,

ANNA DAVIS

Enclosure

Question 1 (from Representative Bass): Does the Federal Trade Commission need additional authority to oversee the practices of charities?

Response. I believe the Commission currently has sufficient authority to combat fraudulent charitable fundraising practices, particularly in light of the additional authority that the new USA PATRIOT ACT of 2001 confers.

Under the Federal Trade Commission Act ("FTC Act"), the agency's mandate is to take action against "unfair or deceptive acts or practices" that are "in or affecting commerce."[1] The FTC Act also equips the FTC with a wide array of tools to enforce this mandate.[2] Sections 4 and 5 of the FTC Act provide the Commission with jurisdiction over corporations only if organized to carry on business for their own profit or that of their members.[3] Over the years, federal courts have construed Section 4 to bar the Commission from suing any truly nonprofit organization under the FTC Act, thereby removing many charitable organizations from the FTC's scope of authority.[4]

Significantly, however, the Commission does have jurisdiction over a nonprofit organization that is merely an instrumentality or a shell used to seek direct monetary gain, either for itself or for its members.[5] The Commission also has jurisdiction under the FTC Act over entities that are organized to carry on business for profit. These entities include for-profit telemarketers, sometimes referred to as "telefunders," that contract with nonprofit organizations to perform the nonprofits' fundraising activities.[6] The Commission has used this jurisdiction aggressively to attack instances of fraud.

The recently-enacted USA PATRIOT ACT of 2001 provides the FTC with an additional tool to address charitable fraud.[7] The USA PATRIOT law amends the statute authorizing the FTC's Telemarketing Sales Rule ("TSR") to apply to certain solicita-

---

[1] 15 U.S.C. § 45(a). The Commission also has responsibilities under more than 45 additional statutes, e.g., the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq., which governs the privacy, fairness, and accuracy of certain sensitive consumer information; the Truth in Lending Act, 15 U.S.C. §§ 1601 et seq., which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 et seq., which provides for the correction of billing errors on credit accounts. The Commission also enforces over 35 rules governing specific industries and practices, e.g., the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[2] These include the authority to file civil actions in federal district court, as well as to bring administrative cease and desist actions, against those who engage in deceptive practices. The FTC Act also enables the Commission to obtain a full range of relief for injured consumers. Typically these civil actions seek preliminary and permanent injunctions to halt the targeted illegal activity, as well as redress for injured consumers.

[3] Section 5(a)(2) of the FTC Act states:

The commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45 (a) (2).

Section 4 defines "Corporation" to include:

any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business for its own profit or that of its members . . . 15 U.S.C. § 44.

[4] *See Community Blood Bank of Kansas City, Inc. v. FTC,* 405 F.2d 1011 (8th Cir. 1969).

[5] *Community Blood Bank,* 405 F.2d at 1019; *Ohio Christian College,* 80 F.T.C. 815 (1972).

[6] *See FTC v. Saja,* 1997-2 Trade Cas. (CCH) ¶ 71,952 (D. Ariz. 1997). *Cf. California Dental Ass'n v. FTC,* 526 U.S. 756 (1999).

[7] USA PATRIOT Act, Pub. Law No. 107-56, §§ 6102(a)(2), (3)(D), 6106(4), __ Stat. __ (2001).

tions of charitable contributions. The Commission is currently considering proposed amendments to the TSR that will implement this new authority.

Acting within the parameters of its authority, the Commission has asserted a strong enforcement presence in the fraudulent fundraising arena. In the past decade, the Commission has filed over 25 cases in federal district courts challenging deceptive fundraising practices by for-profit solicitors. Many of these cases involved "badge fraud," where a telemarketer poses as a law enforcement officer or an affiliate and typically claims that he is raising money to support law enforcement efforts in the donor's local area. In fact, the telemarketer is not a law enforcement officer or affiliate, and the money is not used to support local efforts, as promised. In these cases, the Commission obtained injunctions stopping the deceptive fundraising and, in many cases, recovered monetary redress for consumers.

Question 2 (from Chairman Stearns): Does the Federal Trade Commission wish to be given the authority to develop a national database and corresponding reporting system to track charitable solicitation that occurs in response to national tragedies such as terrorist attacks and natural disasters, similar to the statute that exists in Minnesota?

Response. I am concerned that creating a new, nationwide registration and reporting system to track charities would impose significant costs, that a viable alternative to an FTC-run system might already exist, and that the costs of creating a new system would not outweigh the incremental benefits.

Creating a new registration and reporting system would burden all charities, the vast majority of which are legitimate. With increased administrative costs, charities would have less funds to deliver program services; thus, less of a donor's contribution would go for its intended purpose. Moreover, creating a new system would require significant government resources. For example, many states that have registration requirements have large staffs devoted exclusively to auditing and registration compliance issues.

Notably, an arguably analogous nationwide system is already in place. Currently, in order to obtain tax-exempt status from the Internal Revenue Service, many charities must file with the IRS an application that contains financial statements. In addition, each year, many charities must file a Form 990 return, which requires charities to detail their costs and expenditures and to describe their specific program endeavors. In partnership with the IRS, a private non-profit company, Guidestar, publishes and makes available to the public many of the Form 990 filings that these charities file each year. See www.guidestar.org. In light of the IRS-Guidestar system, it is not clear that the incremental benefits of creating a new FTC-run system would justify the significant additional costs of creating a new system.

Another possible reason to pass new legislation is if it would meaningfully increase the distribution to potential donors of information about charities (whether it be information already collected by the IRS or information that would be collected under the new law). However, the government's ability to require such dissemination is severely constrained by the First Amendment.[8] The Supreme Court has held that charitable fundraising is fully protected speech under the First Amendment. Thus, for example, the government cannot require professional fundraisers to disclose to potential donors the percentage of donations the fundraisers keep,[9] and presumably the government could not require charities that do their own fundraising to disclose the percentage of donations that actually goes to charitable works.

Ultimately, I believe that resources might be better expended targeting law enforcement and regulatory efforts to combat deceptive activity.

Question 3. (from Representative Deal): The safeguards that apply to local pharmacists, in terms of advertising, followup, and counseling, do not appear to apply when consumer purchase prescription drugs online. What is the role of the FTC in the oversight of online pharmacies?

Response. The primary responsibility for the regulation of the dispensing of prescription drugs, both online and offline, is with the state medical and pharmacy licensing boards and the Food and Drug Administration.

The Federal Trade Commission's authority derives from the agency's mandate to prevent deceptive or unfair acts or practices in commerce, pursuant to Section 5 of the Federal Trade Commission Act ("FTC Act").[10] In addition, Section 12 of the FTC

---

[8] Courts have expressly held that enforcing anti-fraud statutes does not violate the First Amendment. *Riley v. National Fed'n of the Blind of N. Carolina,* 487 U.S. 781, 795 (1988). The Commission has successfully argued that false speech, which is the type of speech that the Commission targets for enforcement under Section 5, is not protected by the First Amendment, *Beauhanis v. People,* 343 U.S. 250, 266 (1952).

[9] *Riley,* 487 U.S. at 800.

[10] 15 U.S.C. § 45(a).

Act prohibits the false advertisement of "food, drugs, devices, services, or cosmetics."[11] The marketing of prescription drugs, either online or offline, would be deceptive in violation of the FTC Act if it involved a misrepresentation or omission likely to mislead consumers acting reasonably under the circumstances to their determent. Thus, the Commission has authority to bring an enforcement action where an online pharmacy makes false or misleading claims about the products or services it provides and to obtain injunctive relief prohibiting the entity from making false or misleading claims in the future.

Beginning in 1999, the FTC staff has conducted periodic monitoring of online pharmacy sites, most recently looking at sites selling Cipro (ciprofloxacin) online, to determine whether websites are engaged in deceptive or misleading advertising. The Commission has filed one case against an online pharmacy.[12] In this case, the Commission alleged that defendants falsely represented that their customers were served by a clinic with physicians and an on-site pharmacy. According to the Commission's complaint, defendants' customers were not served by a medical clinic or an on-site pharmacy. Defendants employed one physician in another state to review customers' medical questionnaires. For this service, customers were charged $75.00, if the prescription was approved, and the doctor was paid $10.00 for each of the first 50 prescriptions he approved per week and $7.50 for each additional approved prescription request. The final stipulated order prohibits the defendants' alleged misrepresentations and requires the defendants to clearly and conspicuously disclose certain identifying information to help consumers and state regulatory authorities identify the owners of the website and the pharmacy and physician involved in dispensing the drugs.

As noted above, traditionally, state licensing boards and the Food and Drug Administration have been responsible for regulating the dispensing of prescription drugs. Accordingly, a number of states have actively challenged online companies that dispense prescription drugs without a valid prescription. Kansas,[13] Missouri, and Illinois filed actions against so-called Internet pharmacies, and Michigan issued intent-to-sue letters to 17 sites.[14] The state actions are based on violations of state consumer protection statutes as well as state medical and pharmacy laws. In addition, at least a dozen states have initiated professional disciplinary actions. In one case, an Oregon physician was put on 10 years probation and fined $5,000 for prescribing drugs online without an examination.[15]

Under Federal law, the FDA has regulatory responsibility over prescription drugs. The Federal Food, Drug and Cosmetics Act ("FDC Act") provides that prescription drugs may be dispensed only with a valid prescription under the professional supervision of a physician or other practitioner licensed to administer the drug.[16] A prescription drug dispensed without a valid prescription is "misbranded."[17] The introduction or distribution of misbranded drugs into interstate commerce is prohibited under Section 301(a) of the FDA Act.[18] The FDA may seek injunctive relief to restrain violations of the Act or in appropriate cases pursue criminal charges.[19] FDA can also institute a seizure action under Section 304 of the Act.[20]

---

[11] 15 U.S.C. § 52.

[12] *FTC v. Rennert* (CV-S-00-0861 JBR) (D. Nev.) (July 6, 2000).

[13] *See, e.g., Kansas v. Focus Medical Group, Inc.,* No. 99C749 (D. Kan., Shawnee County, June 9, 1999).

[14] Testimony of Kansas Attorney General Carla J. Stovall before the Health, Education, Labor, & Pensions Committee, Hearing on E-Drugs: Who Regulates Internet Pharmacies, March 21, 2000.

[15] Pittsburgh Post-Gazette, *Internet Viagra,* April 2, 2000, pg. A-12

[16] 21 U.S.C. § 353. In many instances, online pharmacies do not require that the patient have a prior prescription from their treating physician. Patients without a prior prescription can often obtain a prescription online through an "online consultation." These practices raise difficult issues involving physician practices that the Commission traditionally has refrained from regulating.

[17] 21 U.S.C. § 353(b).

[18] 21 U.S.C. § 331(a).

[19] 21 U.S.C. §§ 332, 333.

[20] 21 U.S.C. § 334.

FEDERAL TRADE COMMISSION
BUREAU OF COMPETITION
December 3, 2001

The Honorable EDWARD MARKEY
United States House of Representatives
2108 Rayburn House Office Building
Washington, DC 20515

DEAR REPRESENTATIVE MARKEY: During the recent hearing on "Challenges Facing the Federal Trade Commission" before the House Subcommittee on Commerce, Trade, and Consumer Protection on November 7, 2001, you requested that FTC Chairman Timothy Muris submit a written response detailing the status of compliance with each condition in the America Online/Time Warner (AOL Time Warner) order. Because Chairman Muris is recused from participating in activities associated with the AOL Time Warner matter, he has asked me to respond to your request. As you know, the FTC entered into a consent order with America Online, Inc. and Time Warner, Inc. (Docket No. C-3989), under Section 7 of the Clayton Act, as amended, and Section 5 of the Federal Trade Commission Act, to remedy the likely anticompetitive effects of the merger between the two companies. The consent order, which was finalized on April 18, 2001, sets forth a number of requirements designed to ensure access to the broadband Internet market. The following paragraphs provide an overview of the various requirements in the AOL Time Warner consent order and a summary of the state of compliance by the merged company with each relevant provision.

Paragraph II of the order sets out AOL Time Warner's obligations to make nonaffiliated broadband ISP service available throughout Time Warner Cable's system. Subpart A of this paragraph sets out the requirements as to cable broadband ISP service in each of Time Warner Cable's twenty largest cable divisions. Paragraph II.A.1 of the order requires AOL Time Warner to make Earthlink's ISP service available in each of Time Warner's twenty largest cable divisions no later than AOL Time Warner makes an affiliated ISP service (other than RoadRunner) available in a particular cable division. As of November 30, 2001, AOL Time Warner will have offered its affiliated ISP service in each of Time Warner Cable's twenty largest cable divisions no earlier than it offered Earthlink's broadband service, consistent with its obligations under the order. According to Earthlink's web site, Earthlink is offering its ISP service at a special introductory rate of $41.95 per month. *See* http://www.earthlink.net/home/broadband/cable/tw/availability/ (As of 11/28, service in New York is projected to be available, but not yet available.)

Paragraph II.A.2 of the order requires AOL Time Warner, within ninety days after the affiliated ISP service is made available in each of Time Warner Cable's twenty largest cable divisions, to have entered into agreements approved by the Commission with at least two nonaffiliated ISPs approved by the Commission to make ISP service available in those cable divisions. As of November 30, 2001, AOL Time Warner has entered into such agreements with the following ISPs for the indicated cable divisions (covering all of the twenty largest divisions) and has requested Commission approval of each ISP and each agreement: (1) Juno Online Services Inc. (now merged with NetZero and called United Online) for all cable divisions; (2) High Speed Access Corp. for all cable divisions (application withdrawn); (3) New York Connect for New York City Division; (4) Internet Junction for Tampa Bay and Central Florida Divisions; (5) Inter.net for all cable divisions; (6) STIK for all Texas divisions (San Antonio and Houston); (7) Local.net for upstate New York divisions (Syracuse, Albany, and Rochester); (8) West Central Ohio Internet Link for all Ohio divisions (Columbus, Cincinnati, Western Ohio, and Northeastern Ohio), and (9) Digital Communications Networks (Los Angeles).

Commission staff is currently reviewing AOL Time Warner's requests for approval of the ISPs and the submitted agreements. As part of a review of this kind, staff evaluates the financial and competitive viability of the ISP to determine whether the ISP has the financial capability to implement the agreement and whether it has the experience and expertise necessary to compete in the market. Commission staff reviews financial information concerning the ISP and evaluates its current and proposed business and marketing plans. Commission staff also carefully examines the terms of the proposed agreements to determine whether they are consistent with AOL Time Warner's obligations under the order and whether the agreement enables the ISP to compete effectively in the market or whether any term in the agreement would interfere with the ability of the ISP to compete effectively.

Paragraph II.A.3 of the order gives the Commission the right to appoint a trustee to enter into the required agreements if AOL Time Warner fails to do so within the time limits required. Paragraph III.B of the order sets out the requirements as to

the remainder of Time Warner's cable system (its smaller cable divisions). Paragraph II.B.1 of the order requires AOL Time Warner, within ninety days after affiliated broadband ISP service is made available in each of the remaining divisions of Time Warner Cable's system, to have entered into agreements approved by the Commission with at least three non-affiliated ISPs approved by the Commission to make cable broadband ISP service available in those cable divisions. It is our understanding that AOL Time Warner has not yet launched its cable broadband ISP service in any of these smaller cable divisions, so that the ninety day time period during which it is obligated to make additional ISPs available in these cable divisions has not yet begun. Several of the applications noted above include some of these smaller cable divisions. For example, Inter.net covers all cable divisions; STIK covers Austin; and Local.net covers Binghamton.

Paragraphs II.A.3 and II.B.2 of the order give the Commission the right to appoint a trustee to enter into the required agreements if AOL Time Warner fails to do so within the required time limits. AOL Time Warner is required to have executed agreements with two additional non-affiliated ISPs in the twenty largest cable divisions (and three in the remaining cable divisions) within ninety days after making its own ISP available in a particular cable division. We understand that Earthlink and AOL launched their first cable broadband ISP services in Columbus, Ohio, on September 17, 2001, with launches following in the remaining 19 cable divisions throughout the fall of 2001. AOL Time Warner is thus required to have approved agreements with two additional non-affiliated ISPs in the first cable division by December 16, 2001. If it does not satisfy that obligation, the Commission may at that time determine to appoint a trustee to enter into an agreement, comparable to the Earthlink agreement, with a non-affiliated ISP approved by the Commission.

Subpart C of this section describes specific provisions that must be included in the agreements to be approved by the Commission. The agreements submitted to the Commission for its approval include the specific provisions required by this paragraph of the order. Subpart D of this paragraph describes AOL Time Warner's obligations in the event that an approved ISP ceases providing the service pursuant to the agreement approved by the Commission. No ISP has ceased providing service as of this date. Subpart E of this section requires AOL Time Warner to negotiate and enter into agreements with ISPs to provide cable broadband service on Time Warner's cable system unless certain requirements are satisfied. AOL Time Warner has hired an individual whose primary responsibility includes negotiating with ISPs to provide cable broadband service on Time Warner's cable system in compliance with AOL Time Warner's obligations under the order. Staff of the Compliance Division of the Commission's Bureau of Competition is available to discuss any of the concerns that ISPs might have in connection with this requirement, and members of the staff have had some discussions with ISPs. There is no indication at this point that AOL Time Warner is not complying with its obligation under this provision of the order.

Paragraph III of the order places specific prohibitions on AOL Time Warner in connection with cable broadband service. Subpart A of paragraph HI prohibits AOL Time Warner from interfering with the content of non-affiliated ISPs. Subpart B of paragraph III requires AOL Time Warner to provide connections for the non-affiliated ISPs, at their request, wherever it is providing connections for its affiliated ISP. Subpart C of paragraph III prohibits AOL Time Warner from interfering with the provision of ITV services by non-affiliated ISPs. Subpart D of paragraph III prohibits AOL Time Warner from discriminating against nonaffiliated ISPs in the transmission or modification of the content of the non-affiliated ISPs. Subpart E of paragraph III prohibits AOL Time Warner from entering into exclusive agreements for the provision of ISP services with any other cable company.

Paragraph IV prohibits AOL Time Warner from offering different prices and promotional activities for its cable broadband service based on whether AOL offers broadband DSL service in a particular geographic area. Staff of the Bureau of Competition's Compliance Division monitors AOL Time Warner's compliance with its obligations under these provisions of the order. As part of its monitoring activities, staff talks periodically with non-affiliated ISPs and with representatives of AOL Time Warner, particularly of Time Warner Cable. In addition, staff has made it clear to non-affiliated ISPs that it is available to discuss any concerns the non-affiliated ISPs may have. Staff also consults regularly with Dale Hatfield, the Monitor Trustee in this matter, and he is also available to discuss with any ISPs concerns that they may have and has had on-going discussions with representatives of Time Warner Cable. Staff will continue its normal monitoring procedures, particularly as additional non-affiliated ISP service is made available on Time Warner's cable system.

I hope that the foregoing information addresses your request for a summary of the state of compliance with the AOL/Time Warner consent order.

Sincerely,

JOSEPH J. SIMONS
Director of the Bureau of Competition

Chairman
John T. Dillon
International Paper

Cochairmen
Philip M. Condit
Boeing

Edward B. Rust, Jr.
State Farm

1615 L Street, N.W.
Suite 1100
Washington, D.C. 20036-5610
Tel (202) 872-1260
Fax (202) 466-3509
Web www.brt.org

John J. Castellani
President

Patricia Hanahan Engman
Executive Director

November 7, 2001

Dear Representative:

As Federal Trade Commission Chairman Tim Muris testifies before the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection today, The Business Roundtable is providing committee members with the attached resource entitled *Information Privacy: The Current Legal Regime.*

Last month, Chairman Muris outlined a new privacy agenda that focuses on tougher enforcement of existing laws over the creation of additional privacy legislation. As part of this new agenda, Chairman Muris has called on businesses to develop and implement responsible privacy practices.

The Business Roundtable supports the premise of Chairman Muris' privacy agenda. We believe that the existing privacy laws that are already in place provide a compelling incentive for businesses to establish a responsible approach to information privacy.

To that end, The Business Roundtable has developed *Information Privacy: The Current Legal Regime* as a valuable resource for its members and government officials. This document summarizes the robust body of laws and regulations governing privacy. BRT members have used this resource in assessing their own information collection practices and in developing appropriate privacy practices that instill consumer trust and confidence. We hope this document also will be helpful to lawmakers as you continue to deliberate privacy policy issues.

In addition to distributing informative tools such as *Information Privacy: The Current Legal Regime*, The Business Roundtable has conducted an extensive education program this year to encourage and assist our members in making privacy and security an integral part of corporate culture. For example, The Digital Economy Task Force of The Business Roundtable has hosted a series of seminars in Washington, D.C. and Chicago to provide BRT members with an in-depth understanding of existing privacy laws as well as guidance in establishing and following responsible privacy practices.

We will continue to be active on issues relating to both privacy and security and we look forward to an ongoing, productive dialogue with lawmakers on these important topics. If you have any questions about this report, please contact Bill Sweeney, Vice President of Global Government Affairs at EDS, at (202) 637-6751. Thank you.

Sincerely,

Richard H. Brown
Chairman and CEO, EDS
Chairman, Digital Economy Task Force
The Business Roundtable

Information Privacy: The Current Legal Regime

A Publication of The Business Roundtable
July 2001

Table of Contents

Executive Summary 1

I. Privacy Policies and Unfair and Deceptive Practices 4

II. Federal Laws Applicable to Certain Businesses 5

A. Financial Institutions 6

B. Businesses Subject to FCRA Privacy Provisions 7

C. HIPAA – Health Insurance Portability and Accountability Act of 1996 7

D. Operators of Web Sites Visited by Children 9

E. Additional Federal Laws that May Apply to Online Businesses 9

III. State Law Requirements 10

IV. Considerations for Global Businesses 11

V. Self-Regulatory Initiatives 12

VI. Notice, Choice, Access and Security Requirements of the Significant Current Legal Regimes 13

A. Notice and Disclosure 13

B. Choice and Consent 18

C. Access 22

D. Security 24

Executive Summary

"The two dirty little secrets of the privacy issue are:
privacy is good for business and information sharing is good for consumers."

– Rep. Diana DeGette (D-CO) during a May 8, 2001 hearing in the
House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection

As the issue of information privacy becomes part of the public debate, it is important to understand the substantial body of legal requirements already in place and evaluate the extent to which these rules already address consumer concerns regarding information sharing. The Business Roundtable has prepared this document to summarize the numerous current laws and regulations that make up the current legal regime and provide a strong foundation and incentive for business to provide consumer choice and empowerment.

Companies should use this summary as a reference point for evaluating their obligations and compliance requirements as they change business models to meet consumer and customer demands. At the same time, it is the competitive marketplace environment that provides the most compelling reason for businesses to respond to consumer demands for privacy. Companies that implement a strong corporate privacy policy in response to the marketplace afford themselves a competitive advantage and win business; companies that fail to respond to the marketplace privacy demands will find themselves behind their competitors who do.

It is our hope that lawmakers will use this summary as a reminder of the robust body of law that already governs information practices and protects consumers. Arguably, further legislation and rulemaking will interfere in the efficiency and power of the marketplace and create a patchwork of rules with adverse unintended social and financial consequences. Information privacy is comprehensive and complicated, and all aspects of the existing landscape must be carefully evaluated before considering more governmental involvement in the issue.

The issue of online privacy continues to draw the interest of the public and all levels of government worldwide. Yet there are already in place numerous federal and state laws that serve to protect the privacy and security of the personally identifiable information (PII) of consumers, employees and other customers of companies that collect such data. This survey of the existing laws illustrates the broad landscape of privacy regulation today. These laws and regulations, coupled with market pressure and the use of existing technologies, provide a foundation for U.S. business to embrace a set of privacy principles that should instill even greater trust and confidence.

This quest for consumer trust and confidence has always been a cornerstone of the business model for most companies. This is even more the case in today's digital economy, as both business and consumers grapple with maximizing the dynamic growth of the information and services available. In order to keep up with the changing environment, the private and public sectors are embarking on initiatives addressing consumer and employee empowerment with respect to privacy, including the following:

- Analyzing the impact further or new legislation could have on electronic commerce and the ability of companies to put into place effective self-regulatory rules;
- Examining the use, collection and dissemination of private information;
- Determining the extent to which the use, collection and dissemination is inappropriate;
- Delineating the issue of "opt-in" vs. "opt-out" privacy approaches;
- Examining the possible discriminatory effect of placing unique regulatory burdens on Internet-based activities and subjecting the private sector to different privacy standards than the public sector;
- Determining the extent to which Congress can or should adopt a consistent national standard that avoids conflicting privacy rules; and
- Considering the significant unintended social and financial consequences from further and/or patchwork laws and rulemaking.

Privacy protection is currently governed by a sectoral system of laws, regulations and industry-imposed guidelines. The sectoral framework is based on four widely accepted elements of fair information practices: ***notice, choice, access and security***.

There are at least eleven existing federal laws covering privacy that apply to businesses operating in the United States. While some have been crafted in response to the development of electronic commerce, many of the laws apply equally to any covered information practices, whether they take place online or offline. Therefore, they are of concern to any company involved in these covered information practices.

The most comprehensive and far-reaching privacy protections that have been enacted by Congress include the *Fair Credit Reporting Act* (which protects consumer report information), the Gramm-Leach-Bliley *Financial Modernization Act* of 1999 ("GLBA") (which protects nonpublic personal information collected and used by financial institutions), the *Health Insurance Portability and Accountability Act* of 1996 ("HIPAA") (which protects health information collected by health plans, health care clearinghouses and health care providers), and the *Children's Online Privacy Protection Act* ("COPPA") (which protects personally identifiable information collected from children under 13 years old by operators of Internet websites).

---

2 *The Business Roundtable Digital Economy Task Force*

The U.S. federal government's involvement in privacy also extends to the Federal Trade Commission (FTC), the agency responsible for ensuring consumer protection and market competition. The FTC has sanctioned companies that have violated their own privacy policies, on the basis of those companies having thereby engaged in unfair or deceptive practices, and they will continue to do so under their mandate.

Many states have undertaken their own laws and regulations concerning the confidentiality of certain information about its citizens. If states continue to deal with the privacy issue individually through laws and regulations, they risk worsening this patchwork of rules. This will create considerable confusion as well as direct and indirect costs to businesses to comply – costs that will inevitably be borne by consumers.

Businesses operating in a global framework also face international mandates. Of significant note are privacy rules under a European Union directive concerning the transfer of data. The directive mandates companies engaging in trans-border data flow maintain an "adequate level" of protection for such data.

A powerful alternative to this patchwork of laws and rules is industry self-regulatory initiatives. These range from industry-specific privacy guidelines to online seal programs to high-quality, publicly-posted privacy policies from major corporations. The software industry is also providing consumers with powerful computer tools they can employ to provide them with a technology-based privacy solution that suits their individual needs.

The following summary is an important document that should be read by all companies that share information for marketing, data retention, data mining and other purposes. It is also a valuable resource for government officials, the press and the public who are concerned about information privacy. The Business Roundtable believes that a better understanding of the current, strong legal protections for privacy, and the self-regulatory tools available to companies to fashion a privacy policy in response to marketplace demands, will encourage a responsible approach to information privacy.

---

* While meant to provide an overview of the legal regimes currently in place, this information should be supplemented with a detailed review of the applicable law and regulations as they may apply to a specific company. The legal analysis of any situation depends on a variety of factors that cannot be properly represented or accounted for in the information contained in this document. This information is intended as general information only and is not intended to serve as legal advice or as a substitute for legal counsel.

* This document has been prepared by Marc Pearl, Partner, Shaw Pittman, Legal Counsel to the Digital Economy Task Force of The Business Roundtable.

I. Privacy Policies and Unfair and Deceptive Practices

Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45(a), gives the Federal Trade Commission ("FTC" or the "Commission") broad enforcement authority against businesses that engage in unfair or deceptive acts or practices in or affecting commerce.[1] Certain businesses, including financial institutions (*i.e.*, banks, savings associations and credit unions), common carriers, air carriers, packers and stockyard operators and insurance companies are either wholly or partially exempt from FTC jurisdiction. These entities, however, are regulated by other agencies with authority to enforce compliance with federal law.[2] Under this authority, the FTC has brought numerous enforcement actions against online businesses that have failed to follow a stated privacy policy, or have engaged in conduct that is unfair or deceptive which would require the company to provide notice of such activity to its consumers in the future. Examples of such enforcement actions include:

- **GeoCities** – FTC brought charges against GeoCities, claiming that it had misrepresented the purposes for which it was collecting PII from children and adults through its online membership application form and registration forms for children's activities.
- **Liberty Financial Companies, Inc.** – FTC brought charges against Liberty Financial Companies in connection with its operation of the Young Investor web site, alleging that it had misrepresented that PII collected from children in a survey would be maintained anonymously.
- **Toysmart.com** – FTC brought an action against Toysmart alleging that it had misrepresented to consumers that personal information would never be disclosed to third parties and then disclosing and selling that information to third parties in connection with the company's bankruptcy proceedings.

These and other recent enforcement actions are described further in the attachment. A study of such enforcement actions makes it clear that once a business has communicated its privacy policy to its consumers, any deviation from that policy will most likely be considered a misrepresentation constituting an unfair or deceptive act or practice. Accordingly, any business (online or offline) – regardless of whether notice of its privacy policy is provided *(i) as a voluntary measure to protect consumer privacy, (ii) to comply with an online seal program, (iii) as a result of a recommendation from its insurance carrier, or (iv) if notice is required by statute* – must strictly adhere to the collection, use, access and storage practices that are described to consumers in the business' privacy notice.

[1] In addition to the FTCA, all 50 states have their own unfair and deceptive practice laws that also govern online privacy practices.

[2] *See e.g.*, *In re Providian National Bank*, EA No. 2000-53, 2000 OCC Enf. Dec. LEXIS 54 (OCC Consent Order June 28, 2000) (settlement of OCC enforcement action against Providian National Bank for "misleading and deceptive" practices in violation of the FTCA).

II. Federal Laws Applicable to Certain Businesses

When developing a comprehensive privacy policy, a business must consider whether it engages in a kind of business that is specifically regulated by statutes that have been adopted to protect vulnerable individuals or sensitive data. Statutes that must be considered include:

- Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA") (protects nonpublic personal financial information), 15 U.S.C. §§6801 et seq., Pub. Law No. 106-202, 113 Stat. 1338;
- The Fair Credit Reporting Act ("FCRA") (protects consumer report information), 15 U.S.C. §§1681 et seq.;
- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (protects health information), 42 U.S.C. §1320d;
- The Children's Online Privacy Protection Act, ("COPPA") (protects PII collected from children under 13 years old by online operators of web sites that are directed to children or knowingly collect information from children), 15 U.S.C. §§6501 et seq.;
- The Electronic Communications Privacy Act ("ECPA") (governs electronic communications), 18 U.S.C. §§2510-2522, 2701-2709, 3121-3126;
- The Computer Fraud and Abuse Act ("CFAA") (governs unauthorized access to computer data), 18 U.S.C. §1030;
- The Cable Communications Policy Act of 1984 ("CCPA") (protects personal information collected by cable operators), 47 U.S.C. §551;
- The Federal Videotape Privacy Protection Act ("VPPA") (protects personal information collected by video tape service providers), 18 U.S.C. §2710;
- The Telephone Consumer Protection Act of 1991 ("TCPA") (governs the practices of telemarketers), 47 U.S.C. §227;
- The Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991 ("TCFAP") (expands the protections of the TCPA), 15 U.S.C. §§6101 et seq.; and
- Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (1994) (governs educational institutions' informational records).

The privacy requirements imposed by these and other federal laws that are applicable to businesses engaged in commerce are described more fully in Section VI.

A. Financial Institutions

1. The Gramm-Leach-Bliley Act (GLBA)

Whether operating online or not, businesses that are defined as "financial institutions" by GLBA are subject to the privacy protection regime which took effect on July 1, 2001. GLBA broadly defines financial institution to include any institution whose business is engaging in activities that are "financial in nature." This includes not only banks, savings associations, securities firms and insurance companies, but also mortgage brokers, consumer finance and leasing companies, data processing companies, and even non-financial companies that are "significantly engaged" in financial activities (*e.g.*, a department store that issues a credit card or an automobile manufacturer that provides car loans.) Moreover, any company that receives nonpublic personal information from a financial institution either through an exemption or as a result of a consumer's election not to opt-out of non-affiliate information sharing, is subject to re-use/re-disclosure requirements that generally limit the use of such information to either (i) the purpose for which it was provided; or (ii) only to the extent that the financial institution may legally use the information.

Furthermore, because, under the McCarran-Ferguson Act, individual states regulate the business of insurance, enforcement of GLBA's privacy provisions with respect to insurance companies will be a matter of state law and regulation. Currently, the National Association of Insurance Commissioners (the "NAIC") has promulgated a model rule that may be adopted by the states to implement GLBA (the "NAIC Model Rule").[3] While this rule closely tracks the language of GLBA, it also provides additional protections for health-related information collected by insurance licensees. Section VI highlights significant differences between the NAIC Model Rule and the regulations adopted by the federal agencies under GLBA. The National Conference of Insurance Legislators ("NCOIL") have also adopted a model act concerning privacy of financial information entitled "Financial Information Privacy Protection Act" (the "NCOIL Model Rule"). The NCOIL Model Rule differs from the NAIC Model Rule in two significant respects: (i) the definition of consumer is narrower and (ii) restrictions on health information apply only to sharing information for marketing purposes. States, for which the existing law is not sufficient to comply with GLBA privacy requirements, are free to either adopt their own version of GLBA privacy protections or to adopt the NAIC Model Rule or NCOIL Model Rule in their entirety or with modifications.

The substantive requirements of GLBA call for initial and annual notice, opt-out choice with respect to sharing nonpublic personal information with non-affiliates and reasonable standards for safeguarding consumer information. These requirements are further discussed in Section VI.

---

6 *The Business Roundtable Digital Economy Task Force*

2. OTHER FEDERAL LAWS GOVERNING PRIVACY PROTECTION PRACTICES OF FINANCIAL INSTITUTIONS

The Electronic Funds Transfer Act of 1978 ("EFTA") (15 U.S.C. §§1693 *et seq.*) contains a notice provision designed to protect the confidentiality of information provided in connection with an electronic funds transfer (see discussion under Notice in the attachment). The Fair Credit Billing Act ("FCBA") (15 U.S.C. §§1666 *et seq.*) creates a statutory right to access information in order to challenge the accuracy of information contained in a creditors' file (see discussion under Access in the attachment). Moreover, as discussed below, the privacy protections of FCRA also apply to financial institutions that use consumer report information or that furnish information to consumer reporting agencies.

B. BUSINESSES SUBJECT TO FCRA PRIVACY PROTECTIONS

As discussed in the attachment under "Users of Consumer Reports, Companies that Furnish Information to Consumer Reporting Agencies," companies engaged in such activities, including financial institutions, are subject to the privacy protections of FCRA. FCRA generally limits disclosure of consumer report information to consumer initiated disclosures or other permissible purposes under the FCRA, such as for an extension of credit, employment purposes or underwriting insurance. Subject to certain exceptions, a "consumer report" is any communication of any information that bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, that is collected or used (or expected to be collected or used) as a factor in establishing the consumer's eligibility for credit insurance, employment, or any other permissible purpose under FCRA.

FCRA contains elements of **notice**, **choice** and **access**. The requirements under each of these elements are discussed in Section VI under each applicable element.

C. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

The Secretary of the Department of Health and Human Services has published the "final" Standards for Privacy of Individually Identifiable Health Information (the "HIPAA Rule") to implement the privacy requirements of HIPAA. The rule has been re-opened for public comment and the effective date of the rule has been postponed from February 13, 2001 to April 14, 2001. Compliance with the HIPAA Rule is not mandatory until two years after the effective date (*i.e.*, April 14, 2003).[4]

The HIPAA Rule is an extraordinarily complex regulation with a broad scope that applies to many different entities with access (whether direct or indirect) to personally identifiable health information.[5]

[4] Small health plans have three years from the effective date to comply with the rule.

[5] Given the complexity of the HIPAA Rule, this summary is meant only to provide a broad overview of the rule's privacy protections. Any specific questions concerning the applicability of the HIPAA Rule or its substantive provisions should be raised individually with legal counsel.

More specifically, the HIPAA Rule applies to "covered entities," which include health plans, health care clearinghouses and health care providers who transmit information in an electronic form in connection with a transaction covered by the HIPAA Rule. The scope of the HIPAA rule is further broadened by the definition of "health plan," which is any individual or group plan that provides, or pays the cost of, medical care. The HIPAA Rule therefore applies to group health plans, including most self-insured employee welfare benefit plans that involve the provision of medical care to employees or their dependents directly or through insurance, reimbursement, or otherwise (*i.e.*, any employer that insures the cost of health care for its employees).

The definition of the information protected under the HIPAA Rule ("protected health information" or "PHI") includes all individually identifiable health information ("IIHI") that is transmitted or maintained electronically or in "any form or medium." Accordingly, the HIPAA Rule restricts the use and disclosure of electronic, paper and oral communications.

Under the HIPAA Rule, covered entities may use or disclose PHI (i) pursuant to an individual's authorization; (ii) for treatment, payment or health care operations (if the health care provider has a direct treatment relationship with an individual, the individual's consent must be obtained prior to sharing PHI for these purposes); (iii) by verbal agreement; and (iv) as otherwise permitted under the HIPAA Rule. In addition, when using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request – unless such use or disclosure is for treatment by a health care provider or to an individual.

Furthermore, a covered entity may disclose PHI to a business associate[6] and may allow a business associate to receive PHI on its behalf, if the covered entity obtains satisfactory assurance that the business associate will safeguard the information pursuant a written agreement. The HIPAA Rule contains an exception from the written agreement requirement for disclosures i) by a covered entity to a health care provider and ii) by a group health plan or health insurance issuer or HMO with respect to a group health plan to the plan sponsor, if certain conditions are met. In order to meet the "satisfactory assurance" test, the covered entity must enter into a written agreement that obligates the business associate to abide by the same restrictions on use and disclosure of PHI that covered entities are subject to under the HIPAA Rule.

Although, a business associate is generally only able to use or disclose PHI in a manner allowed by the covered entity, the HIPAA Rule provides two exceptions to allow the business associate to: (i) use or disclose PHI for its own management and administration; and (ii) provide data aggregation

[6] "Business Associates" are defined as entities that receive or use IIHI to perform or assist in the performance of a function or activity on behalf of a covered entity and who provide legal, management or other specified services to entities that involve the disclosure of IIHI.

services relating to health care operations. The substantive requirements of notice, choice, access and security under the HIPAA Rule are described in Section VI.

D. Operators of Web Sites Visited By Children

As set forth above, operators of web sites that are either (i) directed towards children under the age of 13 or (ii) knowingly collect information from children under the age of 13 are subject to the privacy protections mandated by COPPA. COPPA also applies to any entity that engages the service of an online operator to collect information from children on that entities' behalf. The Commission's *Children's Online Privacy Protection Rule* implements COPPA's fair information practice standards. The rule went into effect on April 21, 2000. The rule's protections extend to the collection of information on an operator's web site that is individually identifiable information about a child such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The rule also covers other types of information such as hobbies, interests and information collected through cookies or other types of tracking information when they are tied to individually identifiable information.

In addition to addressing notice, choice, access and security (see attached), COPPA also prohibits operators from conditioning a child's participation in any online activity on the child's providing more information than is reasonably necessary to participate in the activity. COPPA also provides a "safe harbor" for self-regulatory guidelines that implement the protections of the rule that are approved by the Commission.

E. Additional Federal Laws that May Apply to Online Businesses

As set forth above and described more fully in the attachment, additional laws have been enacted that address specific kinds of businesses information collection practices. These laws apply to such businesses as cable operators, videotape service providers and telemarketers of goods and services. Moreover, laws are in place that are meant to protect access and use of computer data, generally and electronic communications (*e.g.*, e-mail). Each of these laws contain some if not all of the four fair information principles and should be considered when developing a comprehensive privacy policy.

Additional federal laws have been enacted that provide general privacy protections in specific areas. For example, the Fair Debt Collection Practices Act prohibits excessive and abusive collection practices that function to limit intrusion on consumers' privacy in debt collectors' contacts with debtors. 15 U.S.C. §§1601 *et seq*. Many federal laws also exist to limit the collection and use of personal information by government agencies. Such laws are outside the scope of this overview.

III. State Law Requirements

States have also adopted, or are in the process of considering, laws meant to protect consumer privacy. Most such laws contain provisions protecting the confidentiality of specific kinds of information (*e.g.*, prohibitions on the disclosure of social security or credit card numbers in certain contexts). Many states also have laws that protect the confidentiality of information provided to state agencies. A full 50-state survey of privacy laws is outside of the scope of this overview. This overview does, however, note where significant state legal requirements for insurance-related information exist.

State common law theories have also been used in private litigation concerning privacy protection. Such theories, while outside of the scope of this overview, include trespass to chattel/personal property and invasion of privacy torts (including misappropriation, public disclosure of private facts and intrusion on seclusion). Moreover, at least one state, California, has a constitutional provision that protects individuals against intrusion on their privacy whether such intrusions are committed by government or private businesses. *CA Constitution – Art. 1, Sec. 1.*

---

10 The Business Roundtable Digital Economy Task Force

IV. Considerations for Global Businesses

The European Commission Directive on Data Protection ("EU Directive")[7] is an essential consideration for any business engaged in activities involving consumer data transfer with European Union-member countries ("EU-member country"). U.S. businesses that have a subsidiary in an EU-member country or whose headquarters are located in an EU-member country must comply with privacy protections set forth under the EU Directive with respect to its business dealings with consumers in EU-member countries. Moreover, under the EU Directive, a business in an EU-member country may not, subject to certain exceptions, engage in cross-border data flows with businesses in non-member countries unless such business maintains an "adequate level" of protection for personal data.

A U.S. company that engages in business with a company operating in an EU-member country that involves the transfer of personal data may volunteer to self-certify that it complies with safe harbor privacy principles negotiated between the European Commission and the U.S. Department of Commerce in order to fulfill the "adequacy" requirement. The U.S. company may choose to apply the safe harbor privacy principles only to consumers from EU-member countries. The safe harbor principles squarely address notice, choice, access and security. A discussion of these requirements is contained in the attachment.

The *Organization for Economic Cooperation and Development* ("OECD") has written a set of privacy guidelines. The OECD privacy guidelines represent the minimum standards that OECD member countries should seek to attain in the protection of personal data whether in the public or private sector. The elements of notice, choice, access and security contained in the OECD privacy guidelines are set forth in the attachment. Businesses may voluntarily choose to follow the OECD privacy guidelines.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281).

V. Self-Regulatory Initiatives

As with the self-regulatory measures that are applicable to businesses with significant operations off-shore, industry self-regulation initiatives play, and should continue to play, a vital role in the development of online privacy policies for all companies that engage in commercial business on the Internet. In an effort to provide comprehensive guidance to online eCommerce participants, many industry groups have established guidelines that expand on the basic fair information principles. See for example, the Online Privacy Alliance's Guidelines for Online Privacy Policies available at: *http://www.privacyalliance.org/resources/ppguidelines.shtml*.

Most significantly, the FTC has endorsed, in the absence of federal legislation governing online profiling, the Network Advertising Initiative's Self-Regulatory Principles Governing Online Preference Marketing by Network Advertisers (the "NAI Principles").[8] In light of the fact that the FTC takes the position that the NAI Principles "serve as the basis for protecting consumer privacy in [the] area [of online profiling]," the NAI Principles are included in the attachment as requirements applicable to companies engaged in network advertising activities.

The primary self-regulatory enforcement initiatives are the online seal programs which require "licensees" to implement certain fair information practices and to submit to various types of compliance monitoring to display a privacy seal on their Web sites. Online seal programs are offered by Truste, BBB Online, CPA WebTrust, Entertainment Software Rating Board, World Wide Web Consortium (WC3), and Individual Reference Service Group. According to the FTC, the online seal programs have not yet established a significant presence on the Web.

In addition to online seal programs, other self-regulatory measures influence online privacy policy. For example, many businesses including IBM, Microsoft, Disney, Intel, Proctor and Gamble, Novell, and Compaq require advertising partners to post high-quality privacy policies.[9] Moreover, software developers are developing privacy protection software that consumers may use to specify their online privacy preferences and avoid web sites that collect PII inconsistent with the stated privacy preference.

---

[8] *See*, FTC Press Release – July 27, 2000 – http://www.ftc.gov/opa/2000/07/onlineprofiling.htm.

[9] *See*, Commissioner Swindle's Dissent *to Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress* (May 2000).

VI. Notice, Choice, Access and Security Requirements of the Significant Current Legal Regimes

A. Notice and Disclosure

Financial Institutions

- A financial institution must provide a "clear and conspicuous" notice to consumers of (i) its privacy policy and (ii) the right to opt out of sharing non-public personal information with non-affiliates. (GLBA)
  - Initial notice must be provided to all consumers (*i.e.*, individuals who obtain a financial product or service from a financial institution) if the financial institution will share the consumers' nonpublic personal information with third party non-affiliates. (GLBA)
  - Initial and annual notice must also be provided to all customers (*i.e.*, consumers who have an ongoing relationship with the financial institution). (GLBA)

- Under GLBA, the privacy policy must include:
  - Categories of information collected.
  - Categories of information disclosed.
  - Types of third parties receiving information.
  - Information-sharing practices for former customers.
  - Categories of information disclosed under the service provider/joint marketing exception.
  - Whether other disclosures to non-affiliated entities are provided as permitted by law.
  - Right to opt out.
  - FCRA disclosures.
  - Disclosures about confidentiality and security of information.

- Financial institutions also must provide notice of the circumstances when deposit or other account information will be disclosed to third parties, including affiliates. (*EFTA*)

Insurance Companies

- The notice requirements of the NAIC Model Rule closely track the notice requirements applicable to other financial institutions except that the NAIC Model Rule requires specific authorizations with respect to nonpublic personal health information. (NAIC Model Rule)
- The Insurance Privacy Act requires insurance companies to provide a notice of information practices to individuals in connection with an application for insurance, a policy renewal, or a policy reinstatement or change in insurance benefits. (IPA)

Health Plans, Health Care Clearinghouses and Health Care Providers ("Covered Entities") (HIPAA)

- Covered Entities who transmit "protected health information" (PHI) (which includes individually identifiable health information (IIHI) as defined by the rule) covered by the rule, must provide individuals with notice describing (i) the uses and disclosures made of their health information and (ii) the individual's rights with respect to those uses and disclosures and how to exercise such rights. The notice must contain, for example, the following:
  - A statement as a header or otherwise prominently displayed that: **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."**;
  - A statement that the Covered Entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;
  - A statement, if applicable, that the Covered Entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains and a description of how it will provide individuals with a revised notice;
  - Information on how to notify the Covered Entity or HHS if an individual believes their privacy rights have been violated including a statement that the individual will not be retaliated against for filing a complaint;
  - A contact person for further information; and
  - The date on which the notice is first in effect (which may not be earlier than the date on which the notice is printed or otherwise published).
- Other than for treatment, payment or health care operations, PHI may be used or disclosed only with the authorization of the individual. The basic form to the authorization must contain for example: (i) name or class of persons authorized to make the requested use or disclosure (ii) description of the PHI to be disclosed; (iii) name of person(s) or class of persons to whom the information will be disclosed; (iv) expiration date or event; (v) statement regarding the individuals right to revoke the authorization; (vi) a statement that information may be re-disclosed by the recipient and no longer subject to the rule; and (vii) signature of the individual authorizing the use or disclosure.
  - If the request for authorization is initiated by the entity (not the individual), the authorization must contain additional statements such as a statement that the Covered Entity may not, in most cases, condition services on the authorization, a description of the purpose for the use/disclosure, whether the entity will gain financially as a result of the use/disclosure and the individual's rights with respect to access to the PHI to be used/disclosed.

- Under some circumstances (see below), PHI may not be used or disclosed without consumer consent. If consumer consent is required, the Covered Entity must provide notice of its privacy practices.
- Special rules concerning the timing and frequency of privacy notices provided by a health plan or a health care provider with a direct treatment relationship also apply under the HIPAA Rule.
- A Covered Entity that maintains a web site that provides information about its customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

Operators of Commercial Web Sites or Online Services that (i) are directed toward children under the age of 13 or (ii) knowingly collect information from children under 13. (COPPA)

- The operators of such web sites must provide a clear and understandable notice that does not include unrelated or confusing material specifying:
  - The name and contact information (address, telephone number and email address) of all operators collecting or maintaining children's personal information through the web site or online service.
  - The kinds of personal information collected from children (*e.g.*, name, address, email address, hobbies, etc.) and how the information is collected — directly from the child or passively (*e.g.*, cookies).
  - How the operator uses the personal information (*e.g.*, marketing back to the child, notifying contest winners, allowing the child to make the information publicly available through a chat room).
  - Whether the operator discloses information collected from children to third parties and, if so, the types of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.
  - That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.
  - That the operator may not require that a child disclose more information than is reasonably necessary to participate in an activity as a condition of participation.
  - The procedures under which the parent can review the child's personal information, ask to have it deleted and refuse to allow any further collection or use of the child's information.[10]
  - The notice must be placed on the operator's homepage (or, if a separate page directed specifically to children exists, on that homepage) in a clear and prominent manner. In addition, the notice must be placed in "close proximity" to any request to obtain information from children.
  - Operators must also make a reasonable effort to provide a separate notice to parents containing the information set forth above.

[10] These requirements and other useful information are provided in the FTC's guide on how to comply with COPPA. Available at: http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm.

Users of Consumer Reports, Companies that Furnish Information to Consumer Reporting Agencies and Consumer Reporting Agencies (FCRA)

- Companies that share "consumer report" information with affiliates must provide consumers with notice and opportunity to opt out of the disclosure to avoid burdensome regulations imposed on consumer reporting agencies.
- A company that offers credit to consumers based on information in consumer reports (*i.e.*, prescreened offers) must provide a clear and conspicuous notice with each offer informing consumers, among other things, as to how they can opt-out of further solicitations.
- A user of an "investigative consumer report" must provide the consumer with a written disclosure that such a report has been requested. The disclosure must include a statement informing the consumer of his/her right to request additional disclosures concerning the nature and scope of the investigation and must include a summary of the consumer's rights.

Companies Engaged in Online Profiling Activities ("network advertisers") (NAI Principles)

- Consumers must receive notice of profiling activities on host web sites.
- If personally identifiable information is collected, the consumer must be notified before personal data is entered. A clear and conspicuous notice in a host web site privacy policy is sufficient to cover the collection of non-personally identifiable information for profiling.

Electronic Communication Service Providers (e.g., email providers) (ECPA)

- Notice is not mandated by statute.

Companies with Access to Computer Data (CFAA)

- Notice is not mandated by statute.

Companies with Large International Operations

- Safe harbor privacy principles require an organization to inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with inquiries or complaints, the types of third parties to which it discloses information, and the choices and means the organization offers individuals for limiting its use and disclosure. (EU Directive)
- Purpose Specification Principle — Requires disclosure of the purpose for which personal data is collected from the individual no later than at the time the data is gathered, and if the purpose subsequently changes, requires the "data controller" (*i.e.*, the party that makes decisions with respect to the content and use of personal data collected) to notify the individual of the changes. (OECD Privacy Guidelines)

---

16 *The Business Roundtable Digital Economy Task Force*

- The Openness Principle data controllers should, among other things, voluntarily publish information concerning the processing of personal data. (OECD Privacy Guidelines)

Notice requirements also exists under:

- The Cable Communications Policy Act of 1984;
- The Federal Videotape Privacy Protection Act;
- The Telephone Consumer Protection Act of 1991 and The Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991.

FTC Enforcement Actions Under Section 5 of the FTCA Concerning Compliance with Privacy Notice

- **GeoCities (February 1999)** – GeoCities agreed to settle FTC charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities.
- **Liberty Financial Companies, Inc. (May 1999)** – Liberty Financial Companies, the operator of Young Investor web site, agreed to settle charges that it had misrepresented that personal information collected from children in a survey would be maintained anonymously. The consent agreement prohibits such misrepresentations in the future and requires Liberty Financial to post a privacy notice on its children's sites and obtain verifiable parental consent before collecting personal identifying information from children.
- **ReverseAuction.com (January 2000)** – FTC filed a complaint against the company claiming that it had improperly obtained the email addresses, user identification names and feedback ratings of various eBay customers. ReverseAuction subsequently settled with the FTC. The settlement bars ReverseAuction from engaging in such unlawful practices in the future. It also requires ReverseAuction to delete the personal information of consumers who received spam mail but declined to register with ReverseAuction and to give those who did register, as a result of the spam, notice of the FTC charges and an opportunity to cancel their registration and have their personal information deleted from ReverseAuction's database.
- **Toysmart.com (July 2000)** – FTC brought an action (that was subsequently settled) in the United States District Court for the District of Massachusetts against the company alleging that it had violated the FTCA by misrepresenting to consumers that personal information would never be disclosed to third parties and then disclosing and selling that information to third parties in connection with the company's bankruptcy proceedings.
- **Pharmaceutical companies (July 2000)** – A group of online pharmacies settled charges brought by the FTC that privacy and confidentiality promises made by the companies were not

upheld. The settlement prohibits the deceptive claims; requires disclosure of medical and pharmaceutical relationships; bars the billing of charge cards without consumer authorization; prohibits disclosure of the information collected from consumers without the consumers' authorization; and, requires them to notify consumers of their practices regarding the collection and use of consumers' personal identifying information.

B. Choice and Consent

Financial Institutions

- A financial institution may not directly or indirectly (through its affiliates) disclose nonpublic personal information about consumers to nonaffiliated third parties unless it has given the consumer a reasonable opportunity to **opt out** of the disclosure. (GLBA)
- The opt out right is not triggered by certain "exempt" disclosures, including disclosure of nonpublic personal information to third party service providers in connection with a joint marketing agreement, for processing and servicing transactions, and certain other disclosures required by law or to protect the financial institution. (GLBA)
- Insurance companies are generally subject to the same requirements as banks with respect to "financial information;" however, the NAIC Model Rule also specifically defines private "health information" and creates a new, affirmative requirement to obtain permission (opt in) before sharing health information.[11]
    - The Insurance Privacy Act generally prohibits the disclosure of personal information except where authorized, in writing, by the individual about whom information is sought or pursuant to an exception provided in the Act. (IPA)

Health Plans, Health Care Clearinghouses and Health Care Providers ("Covered Entities") (HIPAA)

- Covered Entities may, subject to certain exceptions, only use or disclose PHI pursuant to authorization, consent or verbal agreement by the individual. General exceptions to this requirement are based on a variety of public policy purposes, including research, law enforcement, public health activities, emergencies and other purposes required by law.

With respect to **consent**:

- Consent must be obtained prior to using/disclosing PHI to carry out treatment, payment or health care operations;
- An individual may revoke consent;
- A Covered Entity may condition treatment for the health care provider or enrollment in the health care plan on the individual's consent;

[11]The NAIC Model Rule provides a safe harbor for licensees who comply with the regulations promulgated under HIPAA (see discussion under health care providers, etc.).

- Consent is not required if a health care provider has (i) an indirect treatment relationship with the individual; or (ii) created or received the PHI in the course of providing health care to an individual who is an inmate; and
- Consent also is not required in certain emergency treatment situations or when a health care provider has attempted to obtain consent but is unable to do so.

With respect to **authorization:**

- Except in limited circumstances, the Covered Entity **cannot** condition treatment, payment or enrollment in a health plan on an individual's authorization to disclose PHI.

Covered Entities must obtain authorization to use/disclose PHI for marketing purposes (*i.e.*, a communication about a product or service, serving the purpose of encouraging the individual to purchase or use the product or service) unless the communication: (i) is made face-to-face; (ii) concerning products or services of nominal value; (iii) that concern health related products of covered entity or a third party so long as certain conditions are met (opportunity to opt-out must be provided).

- Specifically excluded from the definition of marketing are communications made orally or — if the Covered Entity does not receive remuneration from a third party to make such a communication — in writing, and where the communication is made (i) to describe the entities participating in the health care provider or plan network or the covered products or services provided by the covered entity or included in a plan of benefits; (ii) by a health care provider and tailored to circumstances of a particular individual as part of or in furtherance of treatment; or (iii) by a health care provider or health plan and tailored to the circumstances of an individual in the course of managing the treatment of that individual or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers or setting of care.

Operators of Commercial Web Sites or Online Services that (i) are directed toward children under the age of 13 or (ii) knowingly collect information from children under 13. (COPPA)
Verifiable consent must be obtained from parents for the collection, use or disclosure of personal information from children.

Prior parental consent is not required when an operator collects:

- a child's or parent's email address to provide notice and seek consent;
- an email address to respond to a one-time request from a child and then deletes it;
- an email address to respond more than once to a specific request (the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child);

- a child's name or online contact information to protect the safety of a child who is participating on the site (the operator must notify the parent and give him or her the opportunity to prevent further use of the information); and
- a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose.

Users of Consumer Reports, Companies that Furnish Information to Consumer Reporting Agencies and Consumer Reporting Agencies (FCRA)

- FCRA generally limits disclosure of consumer report information to consumer initiated disclosures or other permissible purposes under the FCRA, such as for an extension of credit, employment purposes or underwriting insurance.
- A user of consumer report information generally may not disclose consumer report information to its affiliates unless it has given the consumer a reasonable opportunity to opt out of the disclosure.
- There are no restrictions on sharing transaction and experience information.
- In a prescreened offer, consumers must be given the right to opt out of further prescreened solicitations.
- A consumer reporting agency may not give out information about consumers to an employer or a prospective employer without first obtaining written consumer consent.
- A consumer reporting agency may not report medical information about a consumer to creditors, insurers, or employers without the consumer's permission.

Companies Engaged in Online Profiling Activities ("network advertisers") (NAI Principles)

- Any linkage of previously collected non-personally identifiable data to personally identifiable data cannot take place without the consumer's affirmative consent (opt in).
- An opt out choice is required for prospective uses of personally identifiable information and the use of non-personally identifiable data.

Electronic Communication Service Providers (e.g., e-mail providers) (ECPA)

- An electronic communication service provider must obtain consent before disclosing the contents of a communication maintained or stored on its system.

Companies with Access to Computer Data

- The ECPA makes it unlawful for anyone to intentionally access stored electronic or wire communications without authorization. Moreover, it is also unlawful to intentionally access stored electronic or wire communications beyond the scope of any given authorization.

- Accessing a computer without authorization or exceeding authorization to access a computer is a crime. (CFAA)

Companies with Large International Operations

- Under the EU Directive safe harbor principles, an organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party (including affiliates), unless such third party is acting as an agent on behalf of an organization or (ii) to be used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. (EU Directive)
- Subject to certain exceptions, an organization must offer an affirmative or explicit (opt in) choice in connection with the sharing of "sensitive information" with third parties under the safe harbor principles (including affiliates). (EU Directive)
    - Sensitive information is generally defined as information pertaining to medical, health, racial/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of an individual.

The OECD Privacy Guidelines provide for individual consent with respect to both the collection and use of data:

- Collection Limitation Principle – Requires that data be obtained by lawful and fair means and with either the knowledge or consent of the individual. (OECD Privacy Guidelines)
- Although the OECD wanted to limit the collection of "specially sensitive" information, it could not reach a consensus as to the definition of "sensitive data." Accordingly, the Collection Limitation Principle contains a general statement that there should be limits to the collection of personal data and includes among the nature of the limitations: (i) data quality aspects, (ii) limits associated with the processing of data; and (iii) civil rights concerns. (OECD Privacy Guidelines)
- Use Limitation Principle – Personal data should not be disclosed or otherwise made available for purposes other than those previously disclosed without the consent of the individual or under the authority of law, including pursuant to licenses granted by a regulatory or supervisory agency. (OECD Privacy Guidelines)

Choice requirements also exist under:

- The Cable Communications Policy Act of 1984;
- The Federal Videotape Privacy Protection Act;
- The Telephone Consumer Protection Act of 1991 and The Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991.

C. Access

Financial Institutions

- The FCBA creates a statutory right to access information in order to challenge the accuracy of information contained in a creditors' file.
- Insurance Companies – The Insurance Privacy Act permits individuals to obtain personal information recorded by the insurance institution and creates a statutory right to challenge the accuracy of personal information maintained by the insurance institution and, where necessary correct, amend, or delete incorrect information. (IPA)

Health Plans, Health Care Clearinghouses and Health Care Providers ("Covered Entities") (HIPAA)

- The rule grants individuals substantial rights to see what PHI in a designated record set about them is maintained by the Covered Entity;
- Individuals may request that the Covered Entity restrict the disclosure of their PHI beyond the restrictions required by law; however, a Covered Entity is not required to honor such requests;
- Individuals must be given the opportunity to inspect and obtain a copy of their PHI in designated record sets, (with limited exceptions);
- Individuals may request amendment or correction of PHI that is inaccurate or incomplete; and
- Individuals must be provided with an accounting of certain disclosures of their PHI to third parties.

Operators of Commercial Web Sites or Online Services that (i) are directed toward children under the age of 13 or (ii) knowingly collect information from children under 13. (COPPA)

- Upon request, operators must provide parents with access to specific personal information collected from their children. An operator must use reasonable methods to verify the identity of the parent before providing any personal information concerning a specific child. The parent may revoke consent for further collection or use of information and may request that the information be deleted.

Users of Consumer Reports, Companies that Furnish Information to Consumer Reporting Agencies, and Consumer Reporting Agencies (FCRA)

- Consumer reporting agencies must provide a consumer with access to information in the consumer's credit file and a list of everyone who has requested the file within a specified time period.
- Consumer reporting agencies must investigate items contained in a consumer's file if the consumer informs the agency that the file contains inaccurate information. A consumer reporting agency must remove or correct inaccurate or unverified information from its files.

---

22 *The Business Roundtable Digital Economy Task Force*

- A company that furnishes information to a consumer reporting agency (a "furnisher of information") may not provide information to the consumer reporting agency if it knows (or consciously avoids knowing) such information is inaccurate. A furnisher of information also has a duty to correct and update information that it has determined is incomplete or inaccurate.
- A furnisher of information must conduct an investigation (within a statutorily defined time period of 30 days) into disputed information whenever it receives a notice of dispute from a consumer reporting agency regarding the accuracy or completeness of any information that has been furnished by such entity.

Companies Engaged in Online Profiling Activities ("network advertisers") (NAI Principles)

- Consumers must be given reasonable access to personally identifiable information and other information that is associated with personally identifiable information retained for profiling.

Electronic Communication Service Providers (e.g., e-mail providers) (ECPA)

- No access requirements exist by statute.

Companies with Access to Computer Data (CFAA)

- No access requirements exist by statute.

Companies with Large International Operations

Under the EU Directive safe harbor principles, individuals must have access to personal information about them that the organization holds and be able to correct, amend, or delete that information where it is inaccurate. Access need not be provided where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual would be violated. Organizations are also subject to a separate requirement to take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current. (EU Directive)

The OECD generally regards the right of individuals to access and challenge personal data as perhaps the most important privacy protection safeguard. Accordingly, the OECD Privacy Guidelines include the following principles:

- Openness Principle – Requires a general policy of openness about developments, practices and policies with respect to personal data. In addition, the principle requires that individuals be allowed to obtain information without unreasonable effort or cost.
- Individual Participation Principle – Provides individuals with the right to: (i) verify the existence of information and obtain the information from a "data controller;" (ii) obtain information in a timely fashion, at a reasonable cost, and in a manner that is readily intelligible; and (iii) challenge

data, and if successful, have the data erased, completed or amended. This principle also requires that "data controllers" provide individuals with reasons for denying requests for information.

Access requirements also exist under:

- The Cable Communications Policy Act of 1984.

D. Security

Financial Institutions (GLBA)

- Under GLBA, the banking agencies have adopted guidelines establishing standards for safeguarding customer information. These guidelines require financial institutions to establish an information security program commensurate with the complexity and scope of the institutions' operations, to:
  - identify and assess the risks that may threaten customer information;
  - develop a written plan containing policies and procedures to manage and control the risks;
  - implement and test the plan; and
  - adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.
- Specific security measures that institutions should consider include: (i) access controls on customer information systems to authenticate and permit access; (ii) access restrictions at physical locations containing customer information; (iii) encryption of electronic customer information (including while in transit or in storage); (iv) procedures designed to ensure system modifications are consistent with the information security program; (v) dual control procedures, segregation of duties, and employee background checks; (vi) monitoring systems and procedures to detect actual or attempted attacks or intrusions on customer information systems; (vii) response programs; and (viii) measures to protect against destruction, loss or damage from natural disasters.
- Financial institutions are also charged with a duty to oversee service providers and require, by contract, that service providers implement security measures that safeguard consumer information (does not apply until July 1, 2003 to contracts entered into on or before March 5, 2001).

Health Plans, Health Care Clearinghouses and Health Care Providers ("Covered Entities") (HIPAA)

- Administrative, technical, and physical safeguards must be established for PHI.
- A Covered Entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements under the rule.

- A Covered Entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Covered Entity.
- Business Associates are also required to provide safeguards for the PHI obtained from or received on behalf a Covered Entity.

Operators of Commercial Web Sites or Online Services that (i) are directed toward children under the age of 13 or (ii) knowingly collect information from children under 13. (COPPA)

- Operators are required to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children against loss, misuse, unauthorized access or disclosure.
- Suggested safeguards include: (i) using secure web servers and firewalls; (ii) deleting personal information once it is no longer being used; (iii) limiting employee access to data; (iv) providing employees with data handling training; and (v) carefully screening third parties with whom the operator shares information.

Users of Consumer Reports, Companies that Furnish Information to Consumer Reporting Agencies and Consumer Reporting Agencies (FCRA)

- No security requirements exist by statute.

Companies Engaged in Online Profiling Activities ("network advertisers") (NAI Principles)

- Network advertisers must make reasonable efforts to protect the data they collect for profiling purposes from loss, misuse, alteration, destruction, or improper access.

Electronic Communication Service Providers (e.g., e-mail providers) (ECPA)

- No security requirements exist by statute.

Companies with Access to Computer Data (ECPA) (CFAA)

- No security requirements exist by statute.

Companies with Large International Operations

- Under the EU Directive safe harbor principles, organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse or unauthorized access, disclosure, alteration or destruction.
- The OECD Privacy Guidelines require that personal data in the possession of "data controllers" be protected by reasonable security safeguards against the risk of loss or unauthorized access, destruction, use (copying), modification or disclosure. Security safeguards include physical measures (*e.g.*, locked doors), organizational measures (*e.g.*, access

levels and confidentiality procedures and policies), and informational measures (*e.g.*, encryption). In addition, data that is no longer relevant should be deleted.

Security requirements also exist under:

- The Cable Communications Policy Act of 1984; and
- The Federal Videotape Privacy Protection Act.

---

26 *The Business Roundtable Digital Economy Task Force*