AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE PRIVACY COMMISSION: A COMPLETE EXAMINATION OF PRIVACY PROTECTION

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

APRIL 12, 2000

Serial No. 106–192

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

70–436 DTP WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
LISA SMITH ARAFUNE, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
HEATHER BAILEY, *Professional Staff Member*
BRYAN SISK, *Clerk*
MICHELLE ASH, *Minority Counsel*

CONTENTS

	Page
Hearing held on April 12, 2000	1
Statement of:	
Cate, Professor Fred, professor of law and Harry T. Ice faculty fellow, Indiana University School of Law, Bloomington; Travis Plunkett, legislative director, Consumer Federation of America; Ari Schwartz, policy analyst, Center for Democracy and Technology; and Sandra Parker, esquire, director of government affairs and health policy, Maine Hospital Association	60
Twentyman, Sallie, victim of credit card theft; Robert Douglas, private investigator; and Paul Appelbaum, M.D., chairman, Department of Psychiatry, director, Law and Psychiatry Program, University of Massachusetts Medical School	14
Letters, statements, etc., submitted for the record by:	
Appelbaum, Paul, M.D., chairman, Department of Psychiatry, director, Law and Psychiatry Program, University of Massachusetts Medical School, prepared statement of the American Psychiatric Association	47
Cate, Professor Fred, professor of law and Harry T. Ice faculty fellow, Indiana University School of Law, Bloomington, prepared statement of	62
Douglas, Robert, private investigator, prepared statement of	26
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	3
Hutchinson, Hon. Asa, a Representative in Congress from the State of Arizona, prepared statement of	7
Parker, Sandra, esquire, director of government affairs and health policy, Maine Hospital Association, prepared statement of	106
Plunkett, Travis, legislative director, Consumer Federation of America, prepared statement of	75
Schwartz, Ari, policy analyst, Center for Democracy and Technology, prepared statement of	87
Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of	12
Twentyman, Sallie, victim of credit card theft, prepared statement of	17

THE PRIVACY COMMISSION: A COMPLETE EXAMINATION OF PRIVACY PROTECTION

WEDNESDAY, APRIL 12, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2247, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Turner.

Also present: Representatives Hutchinson and Moran of Virginia.

Staff present: J. Russell George, staff director and chief counsel; Heather Bailey, professional staff member; Bonnie Heald, director of communications; Bryan Sisk, clerk; Ryan McKee, staff assistant; Michael Soon, intern; Kristin Amerling, minority deputy chief counsel; Michelle Ash and Trey Henderson, minority counsels; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

The first Federal Privacy Commission was established in 1977 to examine a similar issue to that being addressed today: How can private information be protected while allowing public access to information that can benefit society?

Today, a few keystrokes on a computer can produce a quantity of information that was unimaginable in 1974. From e-mail and e-commerce to e-government, technology has simplified the way people communicate, shop, and file their income tax returns.

Last year, for example, more than 17 million people spent $20 billion for on-line purchases. At a subcommittee hearing on Monday, IRS Commissioner Charles Rossotti testified that as of March 31, nearly 21 million people had filed their tax returns electronically this year, a 16 percent increase over the same period last year.

The downside of these technological advances is that a vast amount of personal information now flows over the Internet, and all too often, citizens are being victimized. Today names, addresses, Social Security numbers, and credit reports, as well as other personal information, can be bought by nearly anyone who is willing to pay the going rate.

Today the subcommittee will examine this troubling issue and whether the time has come to establish another Federal commission on privacy. I welcome our witnesses, and look forward to their testimony.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS III, VIRGINIA
DAVID M. McINTOSH, INDIANA
PETER SOUDER, INDIANA
CURT SCARBOROUGH, FLORIDA
STEVEN C. LATOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DOOLITTLE, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
TTY (202) 225-6852

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

"Legislative Hearing to Establish the Commission for the Comprehensive Study of Privacy Protection"

OPENING STATEMENT
REPRESENTATIVE STEPHEN HORN (R-CA)
Chairman, Subcommittee on Government Management, Information, and Technology
April 12, 2000

A quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

The first federal privacy commission was established in 1977 to examine a similar issue to that being addressed today: How can private information be protected while allowing public access to information that can benefit society?

Today, a few keystrokes on a computer can produce a quantity of information that was unimaginable in 1974. From e-mail and e-commerce to e-government -- technology has simplified the way people communicate, shop, and file their income tax returns.

Last year, more than 17 million people spent $20 billion for on-line purchases. At a subcommittee hearing on Monday, IRS Commissioner Charles Rossotti testified that as of March 31, nearly 21 million people had filed their tax returns electronically this year, a 16 percent increase over the same period last year.

The downside of these technological advances is that a vast amount of personal information now flows over the Internet. And all too often, citizens are being victimized. Today, names, addresses, social security numbers and credit reports, as well as other personal information, can be bought by nearly anyone who is willing to pay the going rate.

Today, the subcommittee will examine this troubling issue, and whether the time has come to establish another federal commission on privacy. I welcome our witnesses, and look forward to their testimony.

Mr. HORN. Panel one will be Ms. Sally Twentyman, victim of a credit card theft; Mr. Robert Douglas, private investigator; Paul Appelbaum, M.D., chairman of the Department of Psychiatry, director, Law and Psychiatry Program, University of Massachusetts Medical School. If you will come forward.

Let me just say what the ground rules are. We swear in all witnesses, and we would like—we have your statements, they are all very fine, and we would like you to summarize it if you can in 5 minutes, and certainly not more than 10 minutes. Then we will have panel two later. If you would like to stay, we would certainly welcome that in case you have some comments in relationship to panel two.

So if you will stand and raise your right hands, we will give you the oath.

[Witnesses sworn.]

Mr. HORN. The clerk will note all three witnesses affirmed the oath.

Without objection, Mr. Moran will be a member of this panel, and we will have Mr. Moran, the distinguished gentleman from Virginia, to give us an opening statement then.

Mr. MORAN OF VIRGINIA. Well, thank you very much, Mr. Chairman. Chairman Horn and Mr. Turner and the distinguished staff, I am pleased to join with Congressman Hutchinson, who has just arrived, for this hearing on H.R. 4049, the Privacy Commission Act.

As any Member of this House can attest, privacy is an enormous concern to our constituents. We hear about privacy at our town meetings, in our mail, and from so many citizens who are utilizing the new technologies that are driving our economy. Their concerns are valid. People know that their medical data, which is the most personal information about any of us, is increasingly being electronically stored and transmitted.

As the World Wide Web has become commercialized, some companies have developed the means to profile Web users by the sites that they visit. While such profiling is not all that different from what direct marketers have done for many years, the idea of our purchases and shopping habits being profiled in cyberspace is somehow very unsettling to many people, and rightfully so.

Even though many Web sites have moved aggressively to self-regulate and to display very prominent statements about their own privacy rules, concerns among the public have not abated. Public opinion polls are clear that this remains a major issue for the American people.

As serious as these concerns are, however, there is a countervailing danger of overreaction. The U.S. Internet economy is already worth an estimated $350 billion and is a harbinger of the potential in everything from business-to-business transactions, to consumer retail, to financial services across the board. It is transforming our economy. By the end of this year, some 72 million American adults are expected to be on line; that is 35 percent of the American population. The Internet has flourished in the absence of burdensome government regulations or taxation. Given the stakes to our economy and the depth of public concern, it is clear to us that what is needed is a thoughtful, deliberate approach to privacy issues by this Congress.

That is exactly what the Hutchinson-Moran bill provides. It sets up a 17-member commission appointed jointly by the President and the Republican and Democratic leadership of the House to examine any threats that exist to the privacy of Americans and to report back on whether additional legislation is necessary, and if it is, what protections it should contain. It also directs the commission to report on nonlegislative solutions. If self-regulation can be improved, how should industry achieve that objective? It requires an analysis of existing statutes and regulations on privacy, and an analysis of the extent to which any new regulations would impose undue costs or burdens on our economy. I would note that our colleague in the other body, Senator Kohl of Wisconsin, has sponsored similar legislation.

In short, this is a balanced, measured approach to a complex issue that carries big costs to our economy. I commend Mr. Hutchinson for his leadership on it, and I commend you, Chairman Horn, for holding this hearing about it. It is good to see my colleague Mr. Turner as well. We look forward to hearing from our thoughtful witnesses as well.

Thank you, Mr. Chairman.

Mr. HORN. Well, thank you very much for that opening statement.

Mr. Hutchinson is now with us. Without objection, he will be a member of this panel throughout the morning, and with Mr. Turner's consent, Mr. Hutchinson is free to give his opening statement.

Mr. HUTCHINSON. Thank you, Mr. Chairman. I apologize for walking in here a couple of minutes late. I do thank you for conducting this hearing, and I want to thank the ranking member, Mr. Turner, also for his interest and support of this legislation and his participation in this important hearing. I would like permission to submit the written statement for the record.

Mr. HORN. Without objection, it will be inserted at this point.

I might tell all the witnesses, the minute we introduce you, your full statement is in the record, and then we want you to summarize.

Mr. HUTCHINSON. My colleague Mr. Moran, I value his friendship, judgment, and participation on this important issue. He is the cosponsor with me. We are a team on this, and I thank him, and he has really been instrumental in bringing this issue forward.

I just wanted to talk a little bit about how this came about. We all are familiar with the polls that show the No. 1 concern of persons as we go into the next century being that of personal privacy. But to me, it is much more personal than that. During December, during our break, I conducted a 16-county district tour; went through all of the 16 counties in my congressional district, held town meetings, and I came back and sat down in my living room and sort of penciled in what were the major concerns. Really, to my surprise, privacy was right at the top.

We hear the stories of the hill country folks in Arkansas who really believe that they ought to have privacy; many of them moved to the hills for that reason, and they are concerned about the invasion of that privacy. It is really an unprecedented accumulation and transfer of personal information that we see today in our information society.

So I came back with an intent to address that issue. I looked at what is happening in Congress and realized that there is a lot of different bills out there, many of them are good bills, that address privacy concerns, but I think there are about four different approaches to what we should do with privacy issues. First of all, there is the attitude, let us just do something now, regardless of what it is, let's just get something done. The problem is that doing it right sometimes takes more time, more thought, and I think it is more important than doing it quick and simply as a reaction of the pressing need to get something done. So I think that is the wrong approach.

The second approach is let's pass legislation in a narrow area. We have bills that deal with financial records; we have bills that deal with medical privacy issues, and then we have separate bills that deal with on-line privacy. I am really a cosponsor of a number of those bills that I believe are good, and I want to support and push those through the legislative process. It is important that this commission not be used as a means to stop other efforts that are going through, and that is my intent.

But I do believe that there is much more merit, rather than taking a sectarian approach of, you know, let's look at the financial records issue and health care records with the Internet, it is all-encompassing across every sector of our society. We are really different from the European approach that has taken a more comprehensive approach to privacy than we have taken industry by industry, and I think this commission would broaden it up.

The fourth approach is let's leave it to the regulators. Excuse me, that is the third approach. Leave it to the regulators. As a legislator, I don't think that is the best approach. I believe there should be legislative involvement and a legislative discussion of this.

Finally, that leads to the comprehensive commission that Congressman Moran and I are proposing, the structure he has outlined. It is certainly bipartisan. It is designed to conduct hearings across the country. We have set a time limit of 18 months for a report, but it is important to note that they have authority if they deem necessary to issue an interim report prior to that 18 months, because there could be some need in a particular arena to issue an interim report. So it could move quicker than 18 months.

But clearly, I believe that it is responsible, it is workable, and it is comprehensive; it is the right approach to privacy concerns. We have to be realistic this year. I hope that we can pass some other individual bills. But realistically, I believe this is the best thing that we can do this Congress, and the result will be greater protections of our individual freedom.

I yield back.

Mr. HORN. Thank you very much.

[The prepared statement of Hon. Asa Hutchinson follows:]

Prepared Statement of Rep. Asa Hutchinson
Before the Subcommittee on Government Management, Information & Technology

In Support of H.R. 4049, the Privacy Commission Act

April 12, 2000

Mr. Chairman, first let me thank you, the ranking member, Mr. Turner, and the rest of the subcommittee for hosting this hearing on H.R. 4049, the Privacy Commission Act. In addition, I would like to thank all of the panelists who have come here today to share their experiences and viewpoints. I believe this dialogue on H.R. 4049 will be beneficial for increasing public awareness, as well as a good forum for discussing options to prevent the erosion of an individual's privacy.

Americans are increasingly aware and concerned that their personal information is not as secure as they once believed. In fact, in a Wall Street Journal/NBC News poll last fall, loss of personal privacy ranked as the number one concern of Americans as we enter the new century. This poll took on particular importance for me after conducting a 16-county tour through my home district in Northwest Arkansas. I discovered that one of the most pressing concerns for Arkansans was the loss of an individual's privacy as it relates to the Internet, medical records, and finances. During this tour, I talked with seniors, working-aged adults, and young adults, all of whom were unsure as to what personal information was being shared without their knowledge.

While the questions surrounding privacy have circulated for years, recent developments in technology and changes in existing law have brought this issue to the forefront. Currently, 64 million Americans employ the Internet in some capacity every month, and this number is expected to rise. The Internet has proven to be an effective tool for commerce. Financial transactions over the Internet have grown at an astounding rate with 17 million American households spending $20 billion shopping on-line last year. The use of the Internet as a medium

for commercial activities will continue to grow with estimates that by the end of the Year 2000, 56 percent of U.S. companies will sell their products online.

In addition to the Internet, changes in the financial laws and medical practices have removed some of the traditional barriers protecting individuals' privacy. Traditionally, there have been very few protections regarding medical records, and with breakthroughs in genetic testing and the human genome, as well as the increased sharing of information between medical practitioners, pharmaceutical companies, and insurance entities, some consumers have raised concerns about existing privacy practices. The importance of medical privacy to the public is best illustrated by the estimated 45,000 comments which the Department of Health and Human Services received regarding its proposed rule for medical record privacy.

In addition, Americans are concerned about financial privacy. During the waning days of the first session of this Congress, we passed S. 900, the Financial Services Modernization bill. As part of that comprehensive package, we included language establishing new guidelines for financial privacy. Though S. 900 has not been fully implemented, some groups are concerned that this language does not adequately ensure privacy for the individual.

Unfortunately, even with the existing privacy laws, there have been reports of surreptitious collection of consumer data by Internet marketers and questionable distribution of personal information by on-line companies. While the industry is presently attempting to self-regulate through a number of exiting and new self-driven initiatives, there are no uniform standards ensuring individuals' protections. In addition, consumer information -- educational records, driver's license numbers, payment types, library books, subscriptions to magazines, purchases of goods, etc -- has been collected and traded by non-Internet means for years without any clear parameters, which has resulted in such acts as identity theft and fraud.

Finally, as the nation and the world grows increasingly interdependent and more information is shared over the Internet, we are seeing a number of privacy protection initiatives occurring at the state level as well as in the international community. This patchwork of different ideas and policies has resulted in a variety of privacy standards that further confuse the issue.

In contrast to this disjointed approach to privacy protections, I am proposing, along with Representative Jim Moran, the establishment of a seventeen-member commission to study privacy issues in a comprehensive fashion for a period not to exceed 18 months, at which time the commission will return to Congress with a report of its findings. This commission offers the best solution to the complex and ever-changing world of privacy because it will be able to take a holistic approach, instead of a piecemeal one. As the different fields of health care, financial services, Internet, and others begin to converge, the commission can study these changes and offer recommendations and guiding principles that will ensure the highest levels of personal protection, while enabling the sharing of information for legitimate purposes.

Though several of my colleagues have offered different legislative proposals to address personal privacy, H.R. 4049 is the only bill that examines privacy from a comprehensive standpoint. While I am a cosponsor of several of these efforts, I am very concerned that many critical components of privacy will slip through the cracks without Congress first taking a broader look. H.R. 4049, which offers a safety-net approach, will be empowered to examine many of the different initiatives already occurring in Congress, at the agencies, and even in the private sector.

In addition, by creating a commission which will host a series of local summits throughout the United States, the matter of individual privacy and the legitimate sharing of information can be brought outside of the halls of Congress into the homes of the people. The result will be a studied and thorough approach to privacy legislation.

In conclusion, I firmly believe the privacy commission is a responsible and workable approach to address the growing privacy concerns. By creating public awareness, as well as examining and learning from the different ongoing privacy initiatives, Congress has the opportunity to make substantial and responsible gains in the area of individual privacy.

Again, Mr. Chairman, I would like to thank you and all of the committee for taking the time to hold this hearing. I believe this is an issue that the Government Reform Subcommittee on Government Management, Information, and Technology needs to address, and I appreciate your efforts.

Mr. HORN. The gentleman from Texas, the ranking member, Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. I want to commend Mr. Hutchinson and Mr. Moran for their work on this legislation. It is one of the most important issues that we face. As you mentioned, Mr. Hutchinson, the polls clearly indicate that privacy is one of the top concerns of the American people.

I was pleased to join with you as a cosponsor of this bill because I think the commission will create a high profile for the issue and enable us to have a full and open discussion with the American people about these issues so that we can resolve them in the appropriate way.

I was very pleased to hear your comments about your intent with regard to the commission was not to impede the progress of other legislation that we may achieve a bipartisan consensus on during the time that the commission is working. I think the commission can be a sounding board for a lot of those proposals. I know there are regulations at HHS pending on medical privacy. I hope that the commission would not impede those regulations, but also provide a sounding board for those regulations, because some of these privacy issues need to be dealt with right away. So if we find a consensus on it, and if the agencies are finding their way to protecting our privacy as HHS is trying to do with the medical regulations, I think the American people deserve those protections as soon as possible.

The commission not only can provide a sounding board for the proposals that are out there and for actions that may be taken over the next 18 months, but at the end of the day, hopefully can come up with an overall recommendation in these various areas that represent a true consensus to protect the privacy of the American people.

So I commend you, and I welcome our witnesses here today. We look forward to working on this bill and making it everything that I think the authors intend for it to be.

Thank you, Mr. Chairman.

Mr. HORN. Thank you very much.

[The prepared statement of Hon. Jim Turner follows:]

Statement of the Honorable Jim Turner
GMIT Hearing: H.R. 4049, "To Establish the Commission for Comprehensive Study of Privacy Protection"

Thank you, Mr. Chairman. Over recent years, our country has become more dependent on digital information and the Internet. E Commerce has revolutionized the way we do business. Personal records including medical, financial, purchase, and other information have increasingly been used and transmitted in electronic form. This trend has raised significant privacy issues for many Americans. Recent polls show that the loss of personal privacy is one of the top concerns of Americans. Many consumers believe that businesses ask for too much personal information and feel that they have personally been the victim of a privacy invasion by a business.

Congress has held numerous hearings on and debates on privacy issues. We are here today to examine H.R. 4049, a bipartisan bill which would require the establishment of a 17-member commission. It would be composed of four appointees by the President, four by the majority leader of the Senate, two by the minority leader of the House, and one jointly appointed by the President, majority leader of the Senate, and Speaker of the House. The Commission would be charged with studying "issues relating to the protection of individual privacy and the balance to be achieved between protecting individual privacy and allowing

appropriate uses of information." It would submit a report to Congress and the President within 18 months after the appointment of its members.

Issues that are likely to be addressed at today's hearing include the relationship between the Commission's work and ongoing Congressional efforts to address privacy concerns and how to ensure that Commission members have the appropriate expertise to carry out their mission. While I am pleased to be a cosponsor of this bill, I want to ensure that it does not serve to delay current privacy proposals that are moving toward becoming law. I am interested in hearing from witnesses on how we can ensure that this subcommittee develops the best bill possible.

I want to welcome my colleagues, Asa Hutchison and Jim Moran, and commend them for their bipartisan work on establishing a privacy Commission. We can all agree that Americans deserve a level of protection from privacy invasions. Hopefully, the work of this Commission will lead us to a better understanding of how that can be done. Citizens should not have to live in constant fear of the thought that someone out there might be disseminating our Social Security number, bank accounts, and other pertinent personal information over the information highway for anybody to see. I thank the Chairman for his focus on this issue and welcome the witnesses here today.

Mr. HORN. We will now begin with the first panel. We will start with Ms. Sallie Twentyman, who is the victim of credit card theft. Tell us about it.

STATEMENTS OF SALLIE TWENTYMAN, VICTIM OF CREDIT CARD THEFT; ROBERT DOUGLAS, PRIVATE INVESTIGATOR; AND PAUL APPELBAUM, M.D., CHAIRMAN, DEPARTMENT OF PSYCHIATRY, DIRECTOR, LAW AND PSYCHIATRY PROGRAM, UNIVERSITY OF MASSACHUSETTS MEDICAL SCHOOL

Ms. TWENTYMAN. Mr. Chairman, I do appreciate the opportunity to appear here today to tell you about my experiences.

Last summer my privacy was dealt a blow from which I will never totally recover when I became a victim of identity theft. I still don't know how, when, or where it happened, or who the perpetrator was. I probably never will. But what I do know is that I never received two of my renewal credit cards in the mail, and that someone used my name and Social Security number to access these two credit card accounts and to establish several other new credit card accounts in my name, all in just a matter of a few days and all from a fraudulent address. In one account alone, this person was able to get approximately $13,000 in cash in less than a week.

Over the next several months, this fraudulent activity continued, with my list of residences extending to at least five different States, even after fraud alerts were placed on my name at each of the three credit bureaus in the country.

Today, I am hopeful that the activity is winding down, but I still live each day knowing that my information is in the hands of criminals. This identity theft, especially when perpetrated by a group or a crime ring, as mine probably has been, is similar to what I call financial cancer. Even if, through my efforts, I manage to stop these criminals for a while, they are likely to begin using the information again in the future when they think that I am no longer watching. As identity theft takes new forms, as it does every year or two, I will be at high risk of being a victim of these newer forms of crime.

So far, I haven't been responsible for repaying any of the fraudulent balances, which I appreciate, and I haven't even had pressure put on me, which is good, because I hear a couple of years ago people did have problems with that. I haven't applied for any new loans, so I don't know how difficult it would be to buy a car or get a mortgage at this point or get a student loan to send my teenagers to college, which is coming up in a couple of years.

During the past 8 months, since my identity was stolen, I face some problems and frustrations which I do appreciate being able to come here and tell you about. I faced all of these just as a citizen, a very typical citizen who knew very little about identity theft when it happened to me.

First of all, the Identity Theft and Assumption Deterrence Act made identity theft a crime, and that is very good, but it seems that no one has really been made responsible and are given the manpower needed for apprehending the criminals and enforcing the law. I realize it has kind of skyrocketed, and it is hard for so few people to investigate so many cases.

I was unable to get most law enforcement officials to do anything. When I was unable to get out-of-state police departments to file police reports—because the criminals were very good; they knew to do it in States where I don't live—or to investigate the addresses out of which the thieves were acting, a local police officer made many phone calls for me, but in each case she, too, was unable to get police officials in these other jurisdictions to file reports.

As our country moves from a brick-and-mortar economy to an electronically based economy, law enforcement agencies will need to establish ways of dealing with new electronic forms of crimes which do not fall into specific physical jurisdictions.

I need to note, too, that every governmental agency that I contacted, including the FTC, the FBI, the Secret Service, and the Postal Service, politely took my report, or voice message, or e-mail, and several sincerely wanted to help, I know that they did. However, not a single one ever followed up with me to let me know that they had really done anything with my specific case, which made me—it is very lonely, feeling like nobody is doing anything.

Financial institutions and other businesses need to be made accountable for protecting customers' personal information. Maybe stiff fines and other penalties need to be established when these institutions are negligent or when they continue to open new accounts after fraud alerts have been placed in the person's name. I don't really want to have to get an attorney to do things for me. I really feel they should be made accountable in some way.

My bank did not protect my personal information and helped to spread this financial cancer. In fact, they allowed someone to change my birth date and mother's maiden name in their computers, which made it really hard when I tried to access my account and have something done.

All the banks which issued the fraudulent credit act as if the losses were all theirs; since they wiped my slate clean, I did not owe anything. I would like to point out that their losses were over as soon as they passed on their costs to other consumers in the form of increased service charges and higher interest rates, but my personal information has been lost forever, and I am 44 years old, and there are a lot of years ahead of me.

When a victim learns of his or her identity theft, we need a faster, more effective way of reporting the crime and beginning investigations. The bank told me to start with the credit bureaus, which I did. I left fraud alerts. It was very frustrating, though, getting through voice mails. When you are in shock, when you hear press one of this, two of that, three of that, I had to hang up several times and start over.

Also, it took me 2 weeks to get my credit reports, and during the 2 weeks I just wondered what had been happening, and I wish I could have gotten them sooner. Maybe they could have been faxed to me, e-mailed to me, or something.

I feel we need regulations regarding the issuance of instant credit in this country. These people managed to get instant credit several times, and the bank would call me 3 days later saying, I am sorry, I see we have a fraud alert, but we had issued the credit card, and we will take care of it. But it does keep going on.

We need to also look into the efficacy of establishing some national hotline or fraud reporting agency in some way. I had to report to three different credit bureaus, but not everybody has to check them. Bank accounts who aren't issuing you credit don't have to. I wish there was someplace a victim could call and just put a block on their name totally; no bank accounts, no new cars, no mortgages, nothing without calling me first.

You all are aware of the Internet. I must say that I can look at—I go to Infoseekers.com now, and I see that for $65 they can buy everything about me, my Social Security number, name, address, how many kids I have, what properties I own, medical information. I really wish something could be done. I am not sure, but I will say that that is a sore point for me right now to go on line and see that.

I also recently got an Internet security system and have been having hackers almost daily trying to get in. It has been something.

I know that we need to protect Social Security numbers in the country. I am sure the commission would be looking at who needs it and who doesn't, and restrict it to who does. I don't feel like student IDs, driver's license, medical records, everything has to have Social Security numbers.

Government officials and corporate officials need to really establish ways of authenticating electronic telephone transactions. I know they are doing it, I encourage it. Work diligently, please.

Once again, I do thank you for the opportunity to share my experiences today. I deeply appreciate your efforts in helping to protect the privacy of all citizens.

[The prepared statement of Ms. Twentyman follows:]

Presented by:
Sallie Twentyman
1207 Offutt Drive
Falls Church, VA 22046
Voice: (703) 533-7946
Fax: (703) 532-7040
Email: stwentyman@mgfairfax.rr.com

Presented to:
Congress of the United States
House of Representatives
Committee on Government Reform
Subcommittee on Government Management, Information, and Technology
Legislative Hearing on H.R. 4049

April 12, 2000

I appreciate the opportunity to appear today to report to you my experiences as a victim of identity theft.

Last summer, my privacy was dealt a blow from which I may never totally recover when I became a victim of identity theft. I still don't know how, when, or where it happened, or who the perpetrator was. I probably never will. But what I do know is that I never received two of my renewal credit cards in the mail and that someone used my name and social security number to access these two credit card accounts and to establish several other new credit card accounts in my name—all in just a matter of a few days and all from a fraudulent address. In one account alone, this person was able to get approximately $13,000 in cash in less than one week. Over the next several months, this fraudulent activity continued, with my list of residences extending to at least five different states, even after fraud alerts were placed on my name at each of the three credit bureaus in the country.

Today, I am hopeful that the activity is winding down, but I still live each day knowing that my information is in the hands of criminals. This "identity theft", especially when perpetrated by a group or "crime ring" as mine probably has been, is similar to "financial cancer"—even if, through my efforts, I manage to stop these criminals for a while, they are likely to begin using my personal information again in the future when they think I have relaxed and have quit suspecting them. As identity theft takes new forms, I will be at high risk of being a victim of these newer forms.

So far, I haven't been responsible for repaying any of these fraudulent balances. I haven't applied for new loans, so I don't know how difficult it would be to buy a car or get a mortgage or a student loan to send my teenagers to college.

Many people have written a lot of good material about identity theft, and I will not repeat their work. However, I do want to mention the work of the Privacy Rights Organization and its director, Beth Givens. Their material at www.privacyrights.org helped guide my actions through those first few weeks, and I'm sure that my financial health today would be much worse without their help.

During the past eight months since my identity was "stolen", I faced some problems and frustrations that I would like to share with you. I faced these problems as a typical citizen who knew very little about identity theft before becoming a victim.

1. **The Identity Theft and Assumption Deterrence Act made identity theft a crime, but it seems that no one has been made responsible and/or given the manpower needed for apprehending the criminals and enforcing the law.**

I was unable to get most law enforcement officials to do anything. When I was unable to get out-of-state police departments to file police reports and/or investigate the addresses out of which the thieves were acting, a local police officer made many phone calls for me, but, in each case, she, too, was unable to get police officials to file reports in jurisdictions where the crimes were occurring.

As our country moves from a "brick and mortar" economy to an electronically based economy, law enforcement agencies need to establish ways of dealing with new electronic forms of crimes which do not fall into specific physical jurisdictions.

I need to note, too, that every governmental agency that I contacted (the FTC, the FBI, the Secret Service, and the USPS) politely took my report (or phone voice message or email), and several seemed to want to help. However, not a single one ever followed up with me to let me know whether they have ever taken any action, leaving me feeling that they probably have not.

2. **Financial institutions and other businesses need to be made accountable for protecting their customers' personal information. Stiff fines and/or other penalties may need to be established when these institutions are negligent and/or when they continue to open new accounts after fraud alerts have been placed in the person's name.**

My bank did not protect my personal information and aided in the spread of my "financial cancer". In fact, they allowed someone to change my birthdate and mother's maiden name in their computers, making it very difficult for me to access my own accounts. After I closed the older accounts and opened new accounts, they mailed me the new cards and FedExed a set of these same cards to the fraudulent address

All of the banks which issued me fraudulent credit act as if the losses were all theirs, since they erased the fraudulent transactions from my record. I would like to point out that their losses were over as soon as they passed on their costs to their other consumers

in the form of increased service charges and higher interest rates. My personal information has been lost forever.

3. When a victim learns of his or her identity theft, we need a faster, more effective way of reporting the crime and beginning investigations.

That first day when I learned of my theft, I called the three credit bureaus, placed fraud alerts on my name, and ordered copies of my credit reports. These calls were frustrating. Only TransUnion let me through to talk to someone directly. The other two credit bureaus had me leave voice messages reporting the crime.

When a person discovers that she or he has become the victim of identity theft, he or she needs to talk to someone—a real live person. Voice mail systems should always furnish an option that allows victims to report the theft to a real person—seven days a week. This person should also be able to answer the victim's questions about what steps to take next.

Victims should also have an option of receiving his or her credit reports in a more timely manner. I had to wait for about two weeks to receive my first reports. During this two weeks, I had no idea whmo I should be calling or how extensive the fraud had become. It would have been very helpful if I could have been faxed copies of the report, or could have had them express mailed. More timely delivery of the reports would have lessened the losses by the banks and other financial institutions, as I would have been able to report the incidents of fraud to them two weeks earlier.

4. We need regulations regarding the issuance of "instant credit" in this country.

Two additional bank and credit card accounts have been established in my name since I added fraud alerts to my file at the credit bureaus. Not everyone checks with the credit bureaus before issuing credit. Some issue the "instant" card and check later. A criminal can rack up a lot of charges in the three to four days it takes for a company to check with the credit bureaus retroactively.

5. We need to look into the efficacy of establishing a national hotline/fraud reporting agency in the country.

It would have helped immensely if I had had somewhere to centrally list my name as a fraud victim and that everyone had been responsible for checking (similar to the credit card or check swiping machines) before opening new accounts or making changes to old accounts in my name. For instance, I know that there has been at least one fraudulent checking account established in my name, leaving me wondering how many 1099-INT's went to fraudulent addresses. As it is now, I won't find out about these accounts until problems develop.

6. **Privacy experts need to examine the ways in which the Internet helps to perpetuate this crime.**

Sites such as www.infoseekers.com (see Appendix 1) sell personal information such as social security numbers, addresses, account numbers, and medical records. Any search engine will guide would-be hackers to sites filled with step-by-step instructions on how to hack into personal computers (see Appendix 2). Since loading security software on my personal home computer, I have learned of almost daily attempts by hackers to access the information on this computer (see Appendix 3).

7. **We need to protect individuals' social security numbers in this country, perhaps by establishing a a phase-in period in which social security numbers would be required to be removed as identification numbers for non-governmental use wherever possible (such as on drivers' licenses, medical records, student and insurance ID numbers).**

8. **Government officials, in cooperation with corporate officials, need to work diligently to establish methods for authenticating electronic and telephone transactions.**

Now that so few transactions occur in a face-to-face environment, there need to be ways to verify that the person on the other end of a phone line or from another computer terminal is really the person that he or she claims to be. There has been tremendous progress in the arena of digital signatures, encryption, and other high-tech methods of identification and authentication, and the government needs to do all in its power to see that this progress continues.

Once again, I do thank you for this opportunity to share my experiences and thoughts as the victim of identity theft. I deeply appreciate your efforts in helping to protect the privacy rights of all citizens in this country.

Mr. HORN. Well, thank you for your story. I think it must make every one of us behind this podium and everyone in the seats out there that you just feel like you have been violated, and your whole person is in somebody else's hand and control.

I am going to ask one or two questions now, and then we—we don't want to waste the talent here, and we will do all of them afterwards. But you mentioned the Secret Service. Did you go to the FBI?

Ms. TWENTYMAN. I left a message and was never called back.

Mr. HORN. They never contacted you?

Ms. TWENTYMAN. I think I left two. I never heard back. The Secret Service I did hear from. They asked for some information. I faxed it, but I never heard back. I realize I could have called and really aggressively tried to get, tried harder, but I didn't. I mean, I felt like they knew.

Mr. HORN. Did you contact your own Member of Congress?

Ms. TWENTYMAN. Sitting right over there, I did e-mail him about this.

Mr. HORN. He is the kind of person that gets something done.

Ms. TWENTYMAN. That is right.

Mr. HORN. OK.

Ms. TWENTYMAN. He catches his car thieves, too.

Mr. HORN. I had a problem like that when a few Federal agencies wouldn't move, we just went right to the top, and believe me, they got a little dynamite stick under them and started moving. But that is another story.

Ms. TWENTYMAN. I think part of this is I wanted to also see the citizens—things seem to be winding down. I have been very proactive. I need to observe what is going on, because every citizen does not—I know my parents would not have been extremely assertive. I am just so thankful it is me instead of them and some people.

Mr. HORN. Well, thank you. Stay with us, and we will have some more questions as we finish this panel.

Mr. Robert Douglas is a private investigator. We are glad to have you here.

Mr. DOUGLAS. Thank you, Mr. Chairman. My name is Robert Douglas, and I am the founder of American Privacy Consultants.

I appreciate the opportunity to appear before you in support of the creation of a privacy commission and to state my belief that a comprehensive review of current privacy law and the formulation of a privacy plan for the 21st century are important and long overdue.

Prior to founding APC, I was a Washington, DC, private detective. In 1997, I began investigating the practice of information brokers selling personal financial information. I brought the results of that investigation here to Congress, and I would note in part of that testimony, which I have appended to my statement this morning, I addressed specifically the situation that happened to Ms. Twentyman where her maiden name and birth date records were changed within a financial institution, and I know the techniques that are used to do that, and it happens thousands of times a year around this country.

My 1998 testimony resulted in passage of the Financial Information Privacy Act, which was incorporated in the Gramm-Leach-Bliley financial modernization law.

In 1998, I informed Congress that the use of identity theft, fraud, and deception was rampant in the information broker industry and extended well beyond personal financial information. It is my hope that passage of H.R. 4049 will result in a privacy commission that can act as a small, but very important, part of a broader mandate, to investigate the use of identity theft to access and steal many other types of personal information of citizens and residents of the United States.

I am often asked what personal information can be gathered by the average citizen. The truth is almost anything can be learned about anybody in the United States today. The question is how. The impact of technology on privacy today is the ability to accumulate, store, filter, cross-reference, analyze, and disseminate vast amounts of information about anyone in a fast and cost-efficient manner that was previously unavailable to a point where almost anyone can now afford to participate in the buying or selling of data of any type about anybody. Simply put, privacy in the United States is too often a concept, not a reality.

For the purpose of today's hearing, I would like to focus on several particularly egregious categories of personal information that are being advertised and sold on the World Wide Web. We did have a power point presentation, but I understand it is not able to be done in this room, so if you follow through my statement, I will do the charts that I have there in order.

The first example is found at a company called Docusearch.com, and it is a list of searches. From this menu, one can see that anyone's Social Security number, address, and date of birth can be purchased. These are the essential ingredients for identity theft. With this information, a criminal can impersonate anyone they choose and gain access to all of the personal information concerning the target of the identity theft and do things like happened to Ms. Twentyman. That is how you get in, that is how you change a person's information, that is how you shut off their utilities if you are a stalker or harasser, that is how you steal their finances, that is how you take over their credit history.

The following Web page from Docusearch is the description of the Social Security number search. This page documents—and this is very important—this page documents the use of credit headers for selling personal, biographical information first obtained as part of a normal, ordinary, day-to-day credit transaction and then sold to private investigators and information brokers by our Nation's credit bureaus.

This is a common and widespread practice that must be revisited by Congress. While there are many useful and legitimate reasons for the access of credit header information in certain legal and investigative contexts, the wholesale and unregulated access of biographical data from credit reports goes on at an alarming rate. There are hundreds of Web sites on the Internet, and I repeat hundreds of Web sites on the Internet, selling biographical information obtained from credit reports.

The sale of credit headers is the starting point for many forms of identity theft as it gives the identity thief all of the biographical information necessary to impersonate the true owner of the information. This ability to then impersonate the true owner opens up access to all forms of personal information sought by the identity thief. Congress should extend the same permissible purposes test currently in place for the access to credit data under the Fair Credit Reporting Act to the biographical data included in the credit header, which is now exempted under current interpretations of the FCRA.

The next chart demonstrates another company called Strategic Data Services, and again, we see the sale of Social Security numbers, employment information, dates of birth, driver's license, but added to this we see where they will sell the physical address that goes to a post office box owner, something to someone who has a civil protection order, is trying to stay away from a stalker or a harasser, is terrifying to them, because they will reach out and get and pay extra for a private P.O. box specifically to hide their physical address, and yet here we have hundreds of Web sites selling it. The P.O. box's postal regulations recognize few exceptions for obtaining the corresponding physical address, yet here we see it for sale on the Internet.

The next category shows the sale of driver and vehicle searches, general doc search. Included in the list are the sale of names and addresses associated with a license plate and the sale of a specific driver's license number. So if I see your license plate on your car on the street, and I want to find out who you are and where you live, I can buy that information.

The following Web page shows the specific driver history records by name, and I would note that many Americans believe that the passage of the Drivers' Privacy Protection Act, which I am aware Senator Shelby just held hearings on, I believe, last week, looking to reinforce that act and strengthen it, but I am afraid he missed what I am about to talk about here many Americans believed would stop the sale of this type of information. However, the act allowed an exemption for private investigators. Unfortunately, although there are thousands and thousands of very lawful and upstanding private investigators in this country, there are a number of information brokers who are also private investigators or who have established relationships with private investigators that are subsequently accessing this information and selling it to almost anyone who submits a request on the Internet.

The next page shows telephone searches, and this is an area that I am not aware that anyone in Congress has looked at to this date. One can see from the listing that any phone number can be traced back to its owner. Whether or not the individual owner has taken steps to protect their privacy by again paying extra for an unlisted or nonpublished phone number, it doesn't matter. It doesn't protect you one iota. Again, we have a page demonstrating exactly the sale of nonpublished phone number information.

Again, another page demonstrating all of the other types of phone searches on another Web page, and I will try to move along here for you. But on that one it is very important to note that, in addition to being able to find the ownership site for selling the ac-

tual long-distance toll call records. In other words, you can purchase the long-distance phone records, including the number called, the date, time, and duration of the call. This is actually used in economic espionage, business espionage, on a fairly regular basis in this country.

The next page is, again, financial searches. We can see that even though Gramm-Leach-Bliley was passed last November 12 and signed by President Clinton, that both personal and corporate, private financial information continues to be sold on hundreds of Web sites on the Web. I have documented the specific bank account search here, and there is one portion in the description that I have bolded and underlined that should be alarming to this committee and to Congress, and that is this individual, whose name is Daniel Cohen and operates Docusearch, is claiming that he is accessing a Federal database. The article from Forbes Magazine that I have appended as appendix 1, he goes further in that article and claims he is getting it from the Federal Reserve.

As I pointed out in my speech to the FDIC about 2 weeks ago, I believe that to be a total falsehood. There is no such database with the Federal Reserve. But these are the types of lies these people are telling, even on the Internet, even to reporters like the reporter from Forbes and to our American citizens, which are making our citizens answer the question that Congressman Hutchinson found when he traveled to his district, and I am sure Congressman Moran and others, into believing that they have no longer any financial privacy in this country. They are actually stealing this information through impersonation, but are claiming to our citizens that they have lawful access via Federal databases, and I would hope that that would be of concern to this committee.

The final page is a credit card activity page. To sum that one up, there are dozens of Web sites you can go on where I could buy Ms. Twentyman's actual credit card activity, where she had her dinner, what presents she bought for her family at Christmastime, right down to the individual transactions.

The examples I have provided today demonstrate that a vast and varied amount of personal information is available on the Internet. These examples are just several of thousands available. I have provided committee staff with hundreds of other Web page examples of information being advertised and sold on the Internet, and without saying his or her name, because they asked me not to, I demonstrated to your staff, Chairman Horn, the other day that with one phone call, and I think that person could tell you that, in about 3 minutes I got a phone call back, and I knew her Social Security number and her address. And I have with me a complete report of that individual that I will show them later on today.

If H.R. 4049 passes, and it should, I will do all I can to assist the privacy commission or any committee of Congress to understand and weed out the methods currently being used and developed to access our fellow citizens' personal and private information.

In conclusion, and I apologize for running so long, the time is ripe to have a privacy commission with broad-based authority to

examine privacy in the United States today and to take appropriate steps to safeguard the privacy of all Americans while ensuring that steps are not so Draconian as to impede our booming information age economy. I thank you, Mr. Chairman.

[The prepared statement of Mr. Douglas follows:]

Statement by Robert Douglas

Before the

Committee on Government Reform
Subcommittee on Government Management,
Information and Technology

United States House of Representatives

Hearing On
Establishing a Commission for the Comprehensive
Study of Privacy Protection
H.R. 4049

April 12, 2000

Thank you, Mr. Chairman. My name is Robert Douglas and I am the founder and Chief Privacy Officer of American Privacy Consultants. American Privacy Consultants assists businesses, government agencies, legislators and the media understand and implement appropriate privacy policies and strategies in today's fast changing privacy environment.

First, Mr. Chairman, let me state that I appreciate the opportunity to appear before you to give my support for the creation of a Privacy Commission and to state my belief that a comprehensive review of current privacy law and the formulation of a privacy plan for the 21st Century is important and long overdue. I firmly believe the challenges created by the Information Age to the privacy expectations of our citizens is one of the most significant problems facing our nation today. Striking the right balance between safeguarding the traditional privacy rights and values of all Americans and allowing enough commonsense access to information that is helping the Information Age to thrive will not be an easy task. Nor is it one that should occur on a piecemeal basis. It is time for this country to have a comprehensive privacy plan and strategy.

I want to personally thank you for your willingness and desire to address this serious issue and the time you have invested on this problem. I am aware from both the proposed legislation before us today and other recent activity in Congress that our Nation's representatives have heard the concerns of the American people and are moving to take action. I particularly want to thank your Committee's staff, and specifically Heather Bailey, for the time they have invested with me discussing this problem and assisting me in preparing for my testimony today.

Prior to founding APC, I was a Washington, DC private detective with more than 17 years experience in complex criminal defense investigation and trial preparation. In 1997 after becoming concerned about my own experiences in purchasing personal information

from "Information Brokers" and other private investigators I began investigating the practice of Information Brokers selling citizens personal financial information on the Internet.[1] I took the results of this investigation to Congress and this resulted in my testifying before the Committee on Banking and Financial Services, during the July 28, 1998 Hearing On The Use Of Deceptive Practices To Gain Access To Personal Financial Information. Along with other witnesses I exposed the use of identity theft and fraud by Information Brokers to penetrate banking security systems. That hearing resulted in passage of the Financial Information Privacy Act (FIPA), which was incorporated into the Gramm-Leach-Bliley financial modernization bill signed into law on November 12, 1999.

At the 1998 hearing I informed Congress through the Banking Committee that the use of identity theft, fraud and deception was rampant in the information broker industry and extended well beyond personal financial information.[2] However, given the scope of the Banking Committee's jurisdiction the Financial Information Privacy Act (FIPA) provisions attacking the use of identity theft, fraud and deception under Gramm-Leach-Bliley were narrowly defined and constrained to the illegal access of personal financial information. It is my hope that passage of H.R. 4049 will result in a Privacy Commission that can, as a small but important part of a broader mandate, investigate the use of identity theft to access and steal many other types of personal information of citizens and residents of the United States.

Given my past and current occupations I am often asked what personal information can be gathered about the average citizen. The truth is almost anything can be learned about anybody in the United States today. Name, address, social security number, date of birth, phone number (whether listed, unlisted, or non-published), height, weight, eye color, hair color, mother's maiden name, relatives names and addresses, neighbors names and addresses, criminal records, civil records, tax liens, real estate holdings, bank account numbers and balances, stock holdings, credit card account numbers and individual credit card transactions, long distance phone records, cellular phone records, pager records, 800 number records, motor vehicle records, driving records, aircraft or watercraft ownership, credit histories, medical histories, where you shop and what you buy, where you went to school, what your grades were, even your SAT scores as Vice-President Gore and Governor Bush saw on the front page of the Washington Post.

When I recite that partial list the follow-up question is always; "How?"

The impact of technology on privacy today is the ability to accumulate, store, filter, cross-reference, analyze and disseminate vast amounts of information about anyone in a fast and cost-efficient manner that was previously unavailable. The partial list I provided of the information that can be obtained on anyone has always been available through one means or another. However, until relatively recently this information was rarely accessed to any large degree because of the time and expense that would have been involved in

[1] For an overview of the practices of one Information Broker/Private Investigator see The End Of Privacy, Forbes Magazine, Cover Story, 11/29/99 appended to this statement as Appendix I

[2] July 28, 1998 statement before the Banking Committee appended to this statement as Appendix II

locating it across thousands of different individual computer databases or paper record storage facilities. Today all that information is quickly being accumulated into vast super-databases and is being packaged and sold like any other commodity.

The expanding use of the Internet coupled with decreasing costs and increasing capacity for accumulation and storage of data has brought the information age to a point where almost anyone can now afford to participate in the buying or selling of data of any type about anybody.

Simply put, privacy in the United States is too often a concept not a reality.

For the purpose of today's hearing I would like to focus on several particularly egregious categories of personal information that are being advertised and sold on the World Wide Web. The first example is found at Docusearch.com and is a menu of personal biographical information being sold by a company called Docusearch operating out of the state of Florida.

Locate Searches

PULL DOWN TO DISPLAY HELPFUL INFORMATION -------->

Locate By Social Security Number●

No Hit,
No Fee

43.00

Add

Search For Social Security Number●

No Hit,
No Fee

49.00

Add

Locate By Previous Address●

No Hit,
No Fee

44.00

Add

Search For Date Of Birth

New

25.00

Add

Locate By Name●

No Hit,
No Fee

39.00

Add

Search For Neighbors● NEW!

No Hit,
No Fee

25.00

Add

Locate By Drivers Records NEW!

52.00

Add

Skip Trace For Current Address● NEW!

No Hit,
No Fee

89.00

Add

Current Address From Phone Number● NEW!

No Hit,
No Fee

49.00

Add

●***Premium Search***, Results Are Guaranteed.

From the Locate Searches menu one can easily see that most anyone's Social Security number, address, date of birth and address can be purchased. These are the essential ingredients for identity theft. With this information a criminal can impersonate anyone they choose and gain access to all other personal information concerning the target of the identity theft.

The following web page from the Docusearch site is the description of the Social Security Number Search:

Search For Social Security Number

Search Price
$49.00
Availability
National
Approximate Return Time
1 Business Day

Requires
Subject's full name & complete last known street address

Search Description
This search accesses one national service bureau and is used to locate the Subject's Social Security Number.
Search Strategy
This search should be ordered if you do not know your Subject's Social Security Number, but do possess their first and last name, and a current or previous complete street address. The source of this search is obtained from a major service bureau. We all know that, (with very few exceptions), no matter where you live, maintaining credit is an absolute necessity. The fact that your Subject may have poor credit, is of little consequence. When collection bureaus and skip tracers locate them; they report their findings to the subscribing credit bureau who; in turn, updates the Subject's Credit Header.

No Hit - No Fee

Credit Header
The Credit Header is the top portion of a Credit Report, and details the Subject's current and previous addresses, as reported by participating subscribers as well as the Subject. It usually dates back 7 years or so.
Note: No credit history, ratings, assessments or financial data pertaining to the Subject, will be accessed or returned with search results.
Important Note

There are a couple factors that can reduce your chances of success. One being the accuracy of the submitted information. The slightest inaccuracy will likely return inconclusive results. Another factor is the age of your information. Most credit bureaus purge previous addresses dating prior to 7-10 years.
To gain a greater understanding about Locate Searches, and how to select the one which best serves your specific needs, please review Anatomy of a Locate Search, as well as the additional helpful links provided below.

This page is important because it documents the use of credit headers for obtaining and selling on the Internet personal biographical information first obtained as part of credit transactions and then sold to private investigators and information brokers by credit bureaus. This is a common and widespread practice that must be revisited by Congress. While there are many useful and legitimate reasons for the access of credit header information in certain legal contexts, and despite all intents and purposes of the credit industry, the wholesale access of biographical data maintained as part of credit reports goes on at an alarming rate. There are hundreds of web sites on the Internet selling biographical information obtained from credit reports.

The sale of credit headers is the starting point for many forms of identity theft as it gives the identity thief all the biographical information necessary to impersonate the true owner of the information. This ability to then impersonate the true owner opens up access to all other forms of personal information sought by the identity thief. **Congress should extend the same permissible purposes test currently in place for the access to credit data under the FCRA to the biographical data included in the "credit header" which is now exempted under current interpretations of the FCRA.**

Another company, Strategic Data Service located at Datahawk.com sells similar information:

OTHER GREAT LOCATOR SERVICES

Click here to order!

Locate a person's Social Security #:	**$49**
Locate a person's Current Employer:	**$169**
Locate a person's Date of Birth:	**$69**
Locate a person's Driver's License #:	**$69**
Find physical address of P.O. Box Owner:	**$99**

Again we see the sale of all types of personal information useful for identity theft. Additionally, on the above list we see the sale of the physical street address for a Post Office Box owner. Our citizens pay extra for PO boxes to protect their privacy and U.S. Postal Regulations recognize very few exceptions for obtaining the corresponding physical address. Yet we see it here for sale on the Internet.

The next category shows the sale of Driver and Vehicle Searches at the Docusearch web site. Included in the list are the sale of names and addresses associated with a license plate and the sale of specific driver license numbers. Both pieces of personal information are often used in identity theft.

Driver & Vehicle Searches

PULL DOWN TO DISPLAY HELPFUL INFORMATION -------->

Search Name		Price	Add
Statewide Driver History By Name & License	49 States	39.00	Add
Statewide Driver History By Name & DOB	16 States	39.00	Add
Vehicle Registration Records By Plate or VIN #1	38 States	39.00	Add
Vehicle Registration Records By Plate or VIN #2	9 States	49.00	Add
Vehicle Registration Records By Name/Address	34 States	55.00	Add
Search For Driver License Number NEW!	50 States	52.00	Add

The following web page from the Docusearch site is the description of the Driver History/Records By Name & License Number Search:

Driver History/Records By Name & License Number

Search Price
$39.00

Availability
See Chart

Approximate Return Time
Search results are obtained directly from each state, so return times do vary. The average return time is normally 2-3 business days.

Requires
See Chart

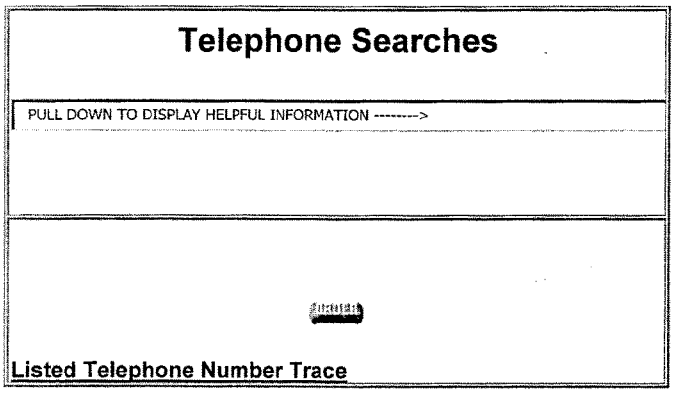
Search Description
Driving Records may provide identifying information and insight into a person's character. It is also useful to determine the status and accuracy of one's own Driving Record, especially when applying for insurance or receiving a ticket, out of State. Information returned may include driver's license number, class and status, full name, date of birth, physical description, dates of convictions, violations and accidents, sections violated, docket numbers, court locations and accident report numbers. Only one State per search will be performed. If the Subject's middle name is recorded on the license, you **must include** the **full middle name** in your request. The middle initial will not suffice.

Note: DMV records are obtained directly from the issuing agency and are subject to local & state laws. Some states restrict access* to the Subject's physical address, and therefore may be omitted. This is out of our control and laws change often and without notice.

*The State of California restricts access and will not return current address information.

Many Americans believe that the passage of the Drivers Privacy Protection Act stopped the sale of this type of information. However, the act allowed an exemption for private investigators. So, as the search description above notes, it is currently left to individual States to regulate the types of information available to private investigators and information brokers. Unfortunately, there are a number of information brokers who are also private investigators, or who have established relationships with private investigators, that are subsequently accessing this information and selling it to almost anyone who submits a request via the Internet.

The next web page category from Docusearch is Telephone Searches:



14.00

☐

Unlisted Telephone Number Trace●

No Hit,
No Fee

49.00

☐

Search For Non-Published Telephone Number●

No Hit,
No Fee

59.00

☐

Disconnected Telephone Number For New Address & Number●

No Hit,
No Fee

89.00

☐

Pager/Beeper Ownership Trace●

No Hit,
No Fee

89.00

☐

Fax Number Ownership Trace●

No Hit,
No Fee

49.00

☐

Cellular Number Ownership Trace●

No Hit,
No Fee

89.00

800/900 Number Ownership Trace●

No Hit,
No Fee

89.00

Pay Telephone Number Trace● NEW!

No Hit,
No Fee

49.00

●***Premium Search***, Results Are Guaranteed.

One can see from this listing that almost any phone number can be traced back to it's owner whether or not the individual owner has taken steps to protect their privacy by paying extra for an unlisted or non-published number.

The next web page is the Search For Non-Published Telephone Number Description from the above Telephone Searches category:

Search For Non-Published Telephone Number

Search Price
$59.00
Availability
National
Approximate Return Time
2-3 Business Days

Requires
Subject's Complete Street Address

Search Description
Given any Subject's complete street address, including zip code and any apartment number, this search will return the Non-Published Telephone Number on record.
Responsible Purpose For Search
This search may return sensitive, confidential, and/or private information. For this reason, DOCUSEARCH.COM requires an explanation stating the purpose for requesting this search, and its' intended use. Additionally, we reserve the right to decline to perform any

search which we deem not to be for a legitimate business purpose or may cause emotional or physical harm.
*Significant restrictions apply

We can see from the description that by just knowing someone's address we can obtain the phone number—even if non-published. This is the type of information that a stalker or harasser uses to chase their prey. While the search description states that a purpose needs to be stated for the request, it is not difficult for someone with criminal intent to make up a reason that will satisfy this requirement.

Again, we find similar services offered by Strategic Data Services:

Unlisted & Unpublished Telephone Numbers, Number Ownership Information, Reverse Number Tracing, Cellular & Pager Telephone Record Searches.

Residential Telephone Number Searches

Description Delivery in business days:	3-5 days	24 hrs	6 hrs
Produce unlisted number from name & address:	$ 65	$119	$169
Produce name & address from unlisted number:	$ 45	$ 99	$149
Produce unlisted number by address only:	$ 99	$149	$199
One month's L.D. calls (dates & numbers called):	$ 99	$149	$199
Call record Extra Detail (Time of day for calls & length)	$ 29	$ 29	$ 29

Click here to order!

Cellular & Pager Searches

Description Delivery in business days:	3-5 days	24 hrs	6 hrs
Produce name and address from cellular number:	$ 99	$149	$199
Produce name & address from pager number:	$129	$179	$229
Produce monthly call records for cellular number:	$149	$219	$249
Call record Extra Detail (Time of day for calls & Length):	$ 29	$ 29	$ 29

However, in the above list we see the addition of long distance toll records. In other words, you can purchase the long distance phone records including the number called, the date, time and duration of the call. Further, there is no requirement for a purpose to be stated.

The next web page category from Docusearch is Financial Searches:

Financial Searches

PULL DOWN TO DISPLAY HELPFUL INFORMATION -------->

National Bankruptcy Filings By SSN

24.00

Statewide Bankruptcy Filings By Name

24.00

Bankruptcy, Tax Liens & Judgments

30 States

29.00

Statewide Debtor Filings

39.00

Current Employment Search●

No Hit,
No Fee

149.00

Bank Account Balance●

No Hit,
No Fee

45.00

Bank Account Search●

No Hit,
No Fee

249.00

Bank Account Activity Detail ● NEW!

No Hit,
No Fee

99.00

Stocks, Bonds & Securities●

No Hit,
No Fee

249.00

Corporate Bank Account Search● NEW!

No Hit,
No Fee

249.00

●***Premium Search***, Results Are Guaranteed.

We can see from this category that both personal and corporate private financial information can be obtained.

The next web page is the description page for Bank Account Searches:

Bank Account Search

Search Price

$249.00
Availability
National
Approximate Return Time
10-18 Business Days*

Requires
Subject's Full Name, Complete Street Address, Social Security Number

Search Description
Given a Subject's full name, complete address and social security number, this search will return the bank name and address, account type, account number, (if available) and approximate current balance of all located personal accounts. ***We access a federal database*** and identify open accounts using the Subject's SSN, however this search will only identify accounts in the Subject's primary state the business resides. If you suspect accounts exist in more than the primary residing state, a separate search request for each state is required, and should include the Subject's address in that state.
NOTE: This search uses the Subject's social security number as the account identifier, so only primary account holders are returned. Also, be sure to include any additional information you may have, such as the Subject's home & work telephone, birthdate, mother's maiden name, etc, in the additional comments section. This will greatly increase the odds of a successful search.
Responsible Purpose For Search
This search may return sensitive, confidential, and/or private information. For this reason, DOCUSEARCH.COM requires an explanation stating the purpose for requesting this search, and its' intended use. Additionally, we reserve the right to decline to perform any search which we deem not to be for a legitimate business purpose or may cause emotional or physical harm.
This is a **Premier Search** and results are guaranteed.
View Sample Report
Important Disclaimer
Financial searches are for informational purposes only, and are not acceptable as an exhibit or as evidence. Every effort is made to provide a complete & thorough search result. However, no method of research is 100% fool-proof and no firm can offer an absolute guarantee that every account will be found.
*This search requires many hours of research and can't be rushed, as we want to return thorough, accurate results. Therefore, this is an **approximate** return time.

Note that under the search description Docusearch claims to be accessing a Federal Database.[3] While I have little doubt that this is a false statement, even if it were true I believe it would be a blatant violation of the Privacy Act. I would also note that even though Gramm-Leach-Bliley and FIPA outlawed certain methods of accessing and

[3] March 23, 2000 remarks before the FDIC Privacy Forum appended to this statement as Appendix III

selling personal financial information, many private investigators and information brokers are ignoring the law or finding other methods of access that they believe fall outside of Gramm-Leach-Bliley.

The next web page description is from Acc-u-data.com and demonstrates the sale of credit card information:

CREDIT CARD ACTIVITY

Scroll Down to Place Your Order

This search will provide you with the monthly credit card bill for either an individual or business. Information required: Full Name, Social SS# or Tax ID#, Street Address, City, State & Zip.

Note you must have a judgement to order this search. That judgement must be faxed to us at 904-532-2981.

Reports are E-Mailed, also the original will be snail mailed along with your paid invoice.

Cost of Search $175.00 Per Statement

While this company appears to require that a judgment be provided in order to obtain a copy of the credit card activity, and it is questionable at best as to whether simply having a judgment in hand would allow lawful access to credit card bills or activity as opposed to a credit report under the Fair Credit Reporting Act, there are many information brokers who make no such requirement. Gramm-Leach-Bliley drove many information brokers underground. However, for the determined individual there are several ways to find brokers who will sell credit card information including individual purchase information.

The examples I have provided easily demonstrate that a vast and varied amount of personal information is available on the Internet. These examples are just several of thousands available. I have provided committee staff with hundreds of other web page examples of information being advertised and sold on the Internet. The methods of access to this data range from lawful collection and resale to illegal theft and resale. I have investigated this issue for the past 4 years. I have worked extensively with the financial services industry and financial regulators to educate and assist them in combating illegal access to financial information. However, that is just a drop in the bucket of the total amount and types of information being accessed.

If H.R. 4049 passes, and it should, I will do all I can to assist the Privacy Commission or any Committee of Congress to understand and weed out the methods currently being used and developed to access our fellow citizens' personal and private information.

In conclusion, the time is right to have a Privacy Commission with broad based authority to examine privacy in the United States today and to take appropriate steps to safeguard the privacy of all Americans while insuring that restrictions are not so draconian as to impede our booming Information Age economy.

Robert Douglas is the founder and Chief Privacy Officer of American Privacy Consultants (APC) located in Alexandria, Virginia, and can be reached at 703-836-8001. APC assists businesses, government agencies, legislators and the media understand and implement appropriate privacy policies and strategies in today's fast changing privacy environment.

Prior to founding APC, Mr. Douglas was a Washington, DC private detective with more than 17 years experience in complex criminal defense investigation and trial preparation. In 1997 Mr. Douglas investigated the practice of "Information Brokers" selling citizens personal financial information on the Internet. Mr. Douglas took the results of this investigation to Congress and this resulted in his testifying before the United States House of Representatives, Committee on Banking and Financial Services, during the July 1998 Hearing On The Use Of Deceptive Practices To Gain Access To Personal Financial Information. Mr. Douglas and other witnesses exposed the use of identity theft and fraud by "Information Brokers" to penetrate banking security systems. That hearing resulted in passage of the Financial Information Privacy Act, which was incorporated into the Gramm-Leach-Bliley financial modernization bill signed into law in November of 1999.

Mr. Douglas and APC continue to monitor the methods of those who would attempt to penetrate our nations financial institutions and violate the privacy of those who entrust their assets to those institutions. Additionally, APC assists financial institutions in developing and implementing programs to prevent the illegal access of depositor's financial information.

Mr. HORN. Well, we thank you a lot, because you have just done a terrific job of taking us through how easy it is to have this happen, and we are indebted to you in terms of the excellent information you provided. I take it you have not ever been filing for Social Security numbers and anything like that. When did you get into this?

Mr. DOUGLAS. I came across it while I was working as an active private investigator in Washington, DC, and started to note that more and more information brokers were advertising in the PI trade magazines, and then relatively blatantly on the Internet. I did attend law school. I had some sense that this could not quite be right, some of the information that they were selling, and I began calling literally dozens of them and actually contracted with a few to find out what types of information they were able to obtain.

Through the course of developing—and they will lie blatantly even to other private investigators, reporters, Members of Congress who have talked to them and claim all types of—you know, it is proprietary databases that we have, investigative sources. And there are certain key phrases that you can find on these Web pages that I could demonstrate to the committee or others, indicate that they are not getting the information legally.

Any time they claim—on the page where they claim they are getting it from a Federal database, well, gee, they are getting it from a Federal database, but on the same page it tells them it takes 18 days to get it. So the reason it takes 10 to 18 days is because what they are doing and what has happened to Mrs. Twentyman is they will buy your credit information, they will then in her case get someone in their office who is female and approximately her age to start calling her bank and calling whatever, the phone company, utility companies, whoever they want to obtain information from and impersonate her, and they now have her name, her date of birth, her address, her Social Security number, and with that information, you can get almost anything, including—and I demonstrated this to Chairman Leach 2 years ago in the Banking Committee. What they do, the way they changed her date of birth and her mother's maiden name—many banks use the mother's maiden name as the password to gain access. I have been advising banks for several years now to change that, and the OCC letter that was put out following my testimony also advised them to go from the maiden name to a PIN number.

Mr. HORN. Explain OCC.

Mr. DOUGLAS. The Office of the Comptroller of the Currency, one of the regulatory bodies overseeing our financial institutions. They put out an advisory letter in the fall of 1998 following my testimony advising them to change that, for the very reason as to what happened to Ms. Twentyman, because here is how it is done. If I want to change your—even your password, I call the bank, and I claim to be Mr. Horn, and I have the biographical data, but maybe I don't have the mother's maiden name. I say, gee, I am on the road, I need to get some information off my checking statement. I am afraid I have a check that is going to bounce. I am out of town. I have to take care of this today. I don't have my checkbook with

me, sometimes they don't have the account number, can you help me.

Well, because in fairness to the banks, they are in the customer service business—and this applies to any other institution, not just financial institutions. They are in the customer service business, they want to be helpful, they are trained to be helpful. So if you have enough data, date of birth, Social Security number, you start to sound real to them. If you have a good enough pretext, as we call it in the industry, falsehood, fraud, and you sound nice enough on the phone, you start to convince them.

Now we get to the tricky question of mother's maiden name. I will say Smith. And the person will say, well, I am sorry, Mr. Horn, that is not what we have here on the account. And excuse me, but the response would be, well, goddamnit, who are you to have the wrong information? I know what my mother's maiden name is. I want a supervisor on the phone right now, or I am pulling my account out of this bank today. Well, hang on, hang on, Mr. Horn, I am sure we can work this out. They eventually convince them that somebody on their end has made a mistake, and then they change Ms. Twentyman's information so that now she cannot even access her own information, but I can.

That is how it is done. It is done dozens of times, if not hundreds of times a day around this country.

Mr. HORN. Well, thank you.

Our last witness on this panel is Dr. Paul Appelbaum, the Chairman of the Department of Psychiatry and Director of the Law and Psychiatry program for the University of Massachusetts Medical School. Thank you for coming.

Mr. APPELBAUM. Thank you, Mr. Chairman. I am Paul Appelbaum, M.D., vice president of the American Psychiatric Association, a medical specialty society representing more than 40,000 psychiatric physicians nationwide. My work treating patients, the empirical studies that I have conducted on medical records privacy, as well as my work consulting with State legislatures, State health agencies, and the U.S. Secret Service have given me a broad perspective on medical privacy issues. Thank you for the opportunity to testify today.

Just a month ago, a leading computer magazine proclaimed in its cover story, we know everything about you. Privacy is dead. Get used to it. I greatly appreciate Representative Hutchinson's and Moran's efforts, as well as the subcommittee's interest, in remedying this loss of privacy.

I focus my comments today on the importance of protecting doctor-patient confidentiality. The level of privacy enjoyed by patients has eroded dramatically, and physicians are often hampered in our ability to provide the highest quality medical care as a result. We have a 21st century health care delivery system, but patients are forced to live with privacy protections designed for the time of Marcus Welby, M.D.

I note for your consideration several examples of today's health privacy crisis. A study by professors at UMass, Harvard, and Stanford revealed over 200 cases where patients at risk for genetic disorders had been harmed by disclosures of medical record information. Patients often forego insurance coverage to maintain their pri-

vacy. I treated a skilled tradesman for 2½ years who worked overtime to pay for his treatment because he didn't want his union, which administered his insurance plan, to know that he was receiving psychiatric care. Members of Congress have seen highly personal disclosures about their medical conditions, some true, some untrue. In one case, a major daily newspaper splashed headlines about a Member's mental health condition only days before the Member's primary. The San Diego Tribune reported that a pharmacy inappropriately disclosed a man's HIV status to his ex-wife, and the woman was able to use that information in a custody dispute.

The Federal Government's appetite for identifiable patient information continues to grow. Witness last year's efforts by HCFA to collect highly personal information in its Oasis program, an effort that they were ultimately compelled, at least partially, to back down from, and how it grows the potential for abuse of this information.

It is critically important to realize that privacy is not only a value in and of itself, it is an essential component of providing the highest quality medical care. Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure of their records. Others simply will not provide the full information necessary for successful treatment, and we know this from a Louis Harris poll that this is a widespread behavior in our society today.

Patients ask us not to include certain information in their medical record for fear that it will be indiscriminately used or disclosed. As a result, more patients do not receive needed care, and the medical records data themselves that we need for many purposes are inaccurate and tainted.

We need a high level of confidentiality protection for all medical records so that all patients receive the privacy necessary for high-quality care. Communicable diseases, mental illness and substance abuse, sexual assault histories, cancer, reproductive and women's health issues, as well as many other conditions may be highly sensitive for patients, and information about these conditions is unlikely to be revealed without assurances that the privacy that exists in the doctor-patient relationship will be maintained.

We believe that many medical privacy proposals before the Congress as well as the regulations being proposed by the Department of Health and Human Services, need to incorporate additional medical privacy protections. The most significant action that Members of this subcommittee can take today to protect medical records privacy would be to contact HHS to express your belief that additional privacy protections should be included in HHS's final regulations, and to conduct hearings on their proposal.

The American Psychiatric Association is very encouraged by Representative Hutchinson's and Moran's privacy commission legislation. Particularly important, in our view, is to focus this proposal on increasing public awareness of the need for additional actions to protect privacy, as well as the actions that citizens can already take to protect their own privacy; working on neglected areas of privacy policy, including the adequacy of privacy protection for employees—many employers have widespread access to their employ-

ees' medical records—and on the Federal Government's use of confidential information; and allowing the current efforts to produce greater privacy to flourish.

We are particularly supportive of the work of the Bipartisan Privacy Caucus led by Representatives Markey and Barton, including legislation introduced to remedy the major financial and medical privacy problems contained in last year's Financial Services Modernization Act.

Last and most important, we believe that all involved parties, whether brick or click private sector companies, privacy experts, consumers, patients and civil libertarians, must be fully involved in the work of a privacy commission. As part of this consensus-oriented approach, we believe it is essential that the membership of any commission contain a balance among all stakeholders, including the privacy community.

Thank you for this opportunity to testify. I look forward to working with the committee on these important issues.

Mr. HORN. Thank you, Dr. Appelbaum.

[The information referred to follows:]

TESTIMONY OF THE

AMERICAN PSYCHIATRIC ASSOCIATION

on

H.R. 4049

TO ESTABLISH A COMMISSION FOR THE

COMPREHENSIVE STUDY OF PRIVACY PROTECTION

before the

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,

INFORMATION AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

PRESENTED BY PAUL APPELBAUM, M.D.

April 12, 2000

Mr. Chairman, I am Paul Appelbaum, M.D., Vice-President of the American Psychiatric Association (APA), a medical specialty society representing more than 40,000 psychiatric physicians nationwide. I Chair the Department of Psychiatry at the University of Massachusetts Medical School, and I know first hand, through my work treating patients, the critical importance of confidentiality to high quality medical care. I would note that the empirical studies on medical records privacy I have performed as well as my work consulting with state legislatures, state health agencies, and the U.S. Secret Service have given me an even broader perspective on medical privacy issues. Thank you Mr. Chairman, Ranking Minority Member Turner, and other Subcommittee members for the opportunity to testify today.

Just a month ago a leading computer magazine proclaimed in its cover story, "We know everything about you....Privacy is dead; get used to it." The loss of privacy is indeed very serious. Privacy and medical records privacy issues are one of the key public policy issues faced by federal and state governments today, and we greatly appreciate Representative Hutchinson's and Moran's efforts as well as the Subcommittee's interest in addressing these issues. We believe it is critically important to protect and to restore many of the privacy protections that, until recently, we enjoyed.

I will focus my comments today on medical privacy issues and the importance of protecting doctor-patient confidentiality. As changes in technology and health care delivery have outpaced the statutory, common law, and other protections that traditionally have ensured patient confidentiality, the level of confidentiality enjoyed by patients has eroded dramatically. We live with a 21st century health care delivery system, but patients are forced to live with privacy protections designed for the 1960's. I will list a sampling of some of the problems that led one national panel of experts to conclude we face a "health privacy crisis."

- A Louis Harris survey reported that 11% of respondents said they or an immediate family member decided to forego insurance reimbursement and pay out of pocket because they feared inappropriate disclosures of medical records information. I would add, unless the public has confidence in our medical system, the accuracy of medical records, including the efficacy of treatment and much health services research, will be tainted by incomplete or false information.

- A study by professors at Harvard and Stanford medical schools revealed over 200 cases where patients had been harmed by disclosures of medical records information.

- Members of Congress have seen highly personal disclosures about their medical conditions, some true, some untrue. In one case a major daily newspaper splashed headlines about a member's mental health condition only days before the member's primary.

- The San Diego Tribune reported that a pharmacy inappropriately disclosed a man's HIV status to his ex-wife, and the woman was able to use that information in a custody dispute. Without their consent patients will receive intrusive calls or letters about the medications they take or marketing-oriented information on their medical condition.

- The federal government's appetite for identifiable patient information continues to grow, and with it, the potential for the abuse of this information.

Confidentiality is a Requirement for High Quality Medical Care

It is critically important to realize that privacy is not only a value in and of itself; it is a critical component of providing the highest quality medical care.

Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure. Some simply will not provide the full information necessary for successful treatment. At other times, physicians are approached by patients who ask us not to include certain information in their medical record for fear that it will be indiscriminately used or disclosed. The result of all these behaviors resulting from patients' reasonable concerns is unfortunate. More patients do not receive needed care, and medical records' data that we need for many purposes is regrettably tainted in ways that we often cannot measure.

Confidentiality is particularly critical for the effective treatment of mental illness. The U.S. Supreme Court recognized the special status of mental health information in its 1996 *Jaffee v. Redmond* decision and ruled that additional protections for mental health information are essential for effective treatment. The Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust…disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment." The 1999 U.S. Surgeon General's Report on Mental Health reinforced this decision. The Report concluded that "people's willingness to seek help is contingent on their confidence that personal revelations of mental distress will not be disclosed without their consent."

Of course a wide variety of medical conditions are sensitive and require the highest level of doctor-patient confidentiality. High blood pressure, communicable diseases, Alzheimer's disease, mental illness and substance abuse, domestic violence, sexual assault information, terminal illnesses, HIV/AIDS, cancer, sexual function or reproductive health issues, as well as many other conditions are highly sensitive. We need a high level of confidentiality protection for all medical records so that all patients receive the privacy necessary for high quality care.

We must enact into law meaningful medical records privacy protections based on the voluntary informed consent of patients and reliance upon the fullest possible use of deidentified and aggregate patient data. In this way the full advantages of patient privacy, as well as the benefits of new medical technology, can be harnessed. As a general principle, the American Medical Association's position -- that patient consent should be required for disclosure of information in the medical record with narrowly drawn and infrequent exceptions permitted for overriding public health purposes -- is eminently reasonable.

We believe that many proposals before the Congress, as well as the regulations being proposed by the Department of Health and Human Services, need to incorporate additional medical privacy protections. For your reference I include a recent editorial from the Journal of the American Medical Association as well as American Psychiatric Association's statement before the Ways and Means Health

Subcommittee that outlines my concerns about these proposals. I encourage members of the Committee to contact the Department of Health and Human Services to express their belief that additional privacy protections should be included in the final proposal, and to conduct hearings on their proposal.

Establishing a Commission for the Comprehensive Study of Privacy Protection

APA is very encouraged by Representative Hutchinson's and Moran's legislation to establish a privacy Commission to study and report on privacy issues. We hope to work with the sponsors of the bill, members of this Subcommittee, and other congressional leaders on privacy issues to establish a federal privacy commission. Particularly important, in our view, is to establish a federal privacy commission that would:

- increase public awareness of the need for additional voluntary, legislative, and regulatory actions to protect privacy as well as the actions that citizens can already take to protect their own privacy.

- focus policymakers on the "neglected" areas of privacy policy, including privacy of information collected or transmitted via the internet, the adequacy of privacy protections for employees, and the federal government's use of confidential information.

As part of the Subcommittee's efforts to craft legislation to develop an effective commission, we believe the Subcommittee should also be mindful of the positive efforts that are already being undertaken by members of the Bipartisan Privacy Caucus headed in the House by Representatives Markey and Barton. We are particularly supportive of their work in the area of financial privacy, including the privacy of medical information maintained by financial entities regulated by the Financial Services Modernization Act. We hope that their efforts will be successful.

We also believe that all involved parties, whether traditional private sector companies, internet and other high-tech firms, financial and medical privacy experts, consumers, patients, civil libertarians and others must be supportive of the establishment of a privacy commission in order for it to operate effectively. Likewise, we believe the findings section of H.R. 4049 should be modified so that the Congress' 1996 decision (contained in the Health Insurance Portability and Accountability Act) to preserve more privacy protective state medical confidentiality laws will not be inadvertently undermined. To maintain a consensus-oriented approach we also believe a commission's membership should have an appropriate balance between all stakeholders, including privacy-oriented stakeholders from the consumer, patient, financial and medical communities. Finally, we would be happy to recommend refinements in the section of the bill delineating the matters that the Committee would report on.

We thank you for this opportunity and we look forward to working with the Committee on these important issues.

Mr. HORN. We are now going to question this panel and we will do it in 5-minute segments, alternating between majority and minority.

Does Mr. Turner want to yield to Mr. Moran, or would you like to start?

Mr. TURNER. I yield to Mr. Moran of Virginia.

Mr. MORAN OF VIRGINIA. Well, thank you, my friend, and thank you, Mr. Chairman, my friend as well. This was very good testimony, and I particularly appreciate my constituent, Ms. Twentyman, to come forward and tell us what happened to you. I know that it is somewhat embarrassing, but I am glad that you have taken the initiative. As you say, I don't know that your mother's generation would be willing to, but you have stepped forward, and I appreciate it.

It is just such a constituent that initiated the Driver's Privacy Protection Act. It was a woman who went to a health center to get advice, she had just had a miscarriage, and by the time she got home, she drove home, she lived in northern Virginia, there was a group picketing on her front lawn because they assumed that she had had an abortion, because that health clinic had also offered a full range of services to women. In addition to being—the irony of it and being distraught, she just couldn't imagine how they had known where she lived, and we found out that what they had done was simply write down the license numbers of the cars and the tag numbers and went to the State Division of Motor Vehicles that was in Alexandria and got the addresses, the names of everyone that had parked in that lot, and that just didn't seem right.

The State was collecting $5 for every individual piece of information, direct marketing organizations, of course, were paying more. We found out that there were a number of organizations that were determined to continue that practice because they made a lot of money off of it, and most protective of that practice was the States. They were making millions, as Mr. Douglas has indicated. But the detectives particularly wanted to be exempted. We exempted them, and I know the newspapers and publishers' associations want to be exempted. I don't think the conference report finally exempted them, but they thought it was also a great idea to be able to access this information.

So we are vulnerable. But it would seem, and I know Asa feels just as strongly, and I suspect my friend Mr. Horn and Mr. Turner do as well, that we should not try to impose a type of cookie cutter approach from the public sector if there is a way that the private sector can regulate itself. There does seem to be a number of initiatives being attempted that would enable you to do that.

I guess I would like to solicit from the three of you, if you have seen ways in which your situation, Ms. Twentyman, could have been avoided, or you could have been protected. Mr. Douglas, this information you give us is just astounding, the access that people can get to our information, and then can shut us off from even getting our own information. Dr. Appelbaum, you have obviously explored this very extensively as well.

Do you see efforts in the private sector developing that are able to self-regulate, or at least give people an option to keep their information private? What we did with the Driver's License Privacy

Protection Act was to require that a box be on the license application that you can't miss if you don't want that information shared, you just check it, and then it is against the law to give out any information on that person's data without that person's permission.

Let me see whether any of the three of you have come across ways that have already developed, nongovernmental ways that might have protected you. Dr. Appelbaum.

Mr. APPELBAUM. The medical information developments in the last several years have resulted in a widespread use of computerized medical records and aggregated databases in ever-growing HMOs and hospital systems. Some of these systems are beginning to pay attention to these issues. For example, I can tell you that at the University of Michigan's Medical Center in Ann Arbor in the last year, having implemented an electronic medical record, they have simultaneously carved out and placed behind a firewall the psychiatric portion of those records, with limited access only to people in the Department of Psychiatry. So such efforts are, indeed, possible.

The problem, I think from my perspective, is that the incentives all push in the other direction in terms of doing things easily, using information for marketing purposes and mining it for additional revenues. The private sector has every incentive not to pay attention to these issues. And though direct regulation may be a last resort, at the very least, I would think that some sort of balancing incentives should be given to these organizations so that they receive some encouragement to take privacy seriously.

Mr. DOUGLAS. I think you hit exactly on what is the main discussion or argument taking place in the business community today, and that is fair information practices and key phrases like opt-in versus opt-out. Currently, the burden is on the consumer, people like Ms. Twentyman, to safeguard their own information. If you were to sit down with a pen and paper and list all of the different places that you have private data, private information, you would still be writing at 5 p.m. So the burden is currently on you as the consumer, as an American citizen, to go out and find all of those places and tell them, if they will even listen to you, that you want to opt out, that you don't want your information being shared.

The discussion today, I know the discussion within the financial community and certainly as we sit here today, the regulators are proposing regulations under Gramm-Leach-Bliley dealing with third party affiliates, opt-in versus opt-out, and it is very cumbersome. The average American consumer is not going to understand it. What many are arguing for today is that it should be opt in. As far as information practices, if I give you—and let me just use the example of the credit agencies, we all have to participate, almost all of us, in credit transactions on a daily basis. But we believe when we fill out a credit application, a mortgage application, a rental application, a department store application, that that information is between us, the credit bureau and the person making the decision as to whether they will grant that credit, but that is not the truth of the matter. The truth of the matter is, through the credit headers and the recompilation in the vast databases, a lot of that statistical information is being resold. Every day your and

my information is running up millions of dollars for American business and the States, as you noted.

As just one afterthought, you had mentioned the Newspaper Guild or somebody's resistance to the DPPA. Deep within the article that I have attached as appendix I from Forbes is a story of a company called Touchtone Services out of Colorado that I am very familiar with, because they are one of the few successful prosecutions of an information broker in this country, and Mr. Rap, who is the owner of that company, I think just got out of jail within the last week or two after serving, what, 70 days.

Let me tell you what he did as part of the allegations. He was selling information on the Cosby family to the tabloids. We often wonder how the newspapers and the TV stations show up on our doorstep when there is a tragedy, like an aircraft crash or something like that, faster than even the police, because they go to these information brokers. They have one on contract, private investigators who know how to use these techniques of how to impersonate people. The Jon-Benet Ramsay, he impersonated Mr. Ramsay and was able to obtain his banking information. He was able to obtain where the Colorado detectives were secreting witnesses and in what hotels.

In the Monica Lewinsky investigation, it was his firm that obtained Kathleen Willey from Richmond's phone records and sold it to a Montgomery County private investigator who turned it over to the attorney of a very prominent Democrat who is still under investigation in an Alexandria grand jury.

Perhaps most egregious of all, and I went over this with your staff the other day, Mr. Horn, he was able to get the pager numbers of undercover LAPD police officers that were working on a very important investigation with the Israeli Mafia and they were able to clone those pagers, a little technical, but there is a way to do that, so that they, the bad guys, were getting the same pages that the undercover officers were getting, and they were then able to figure out who the secret witnesses were in the investigation and get the home addresses of the undercover police officers who, in one case, showed up on the doorstep while the officer was away and intimidated the wife of the officer.

So we are not talking kid's play here. There are very serious things that are going on out there, and it all leads back to how our information is being bought, sold and packaged every day in this country.

Mr. MORAN OF VIRGINIA. Troubling. Thank you, Mr. Douglas.

Mr. HORN. The gentleman from Arkansas, Mr. Hutchinson.

Mr. HUTCHINSON. Thank you, Mr. Chairman. I want to join in the thanks to each of the panelists for your extraordinary testimony today. I want to focus with Mr. Douglas for just a moment. I really do appreciate your expertise. We need to have more people that have a background in the darker, sinister world.

Mr. DOUGLAS. My mother would be so happy to hear that.

Mr. HUTCHINSON. I want to focus on Social Security numbers for just a second. We all have our stories of going into a business and cashing a check and they ask for your Social Security number, sometimes you don't even give them a check, you pay cash for it

and they want to know your address and they want to know information.

Mr. DOUGLAS. Radio Shack, yes.

Mr. HUTCHINSON. Your natural inclination, in the South we are particularly friendly, we just give them what they ask, we are accommodating. Of course, the dissemination of that information is a concern.

But in reference to Social Security numbers, clearly, they are being used far beyond what was originally intended. What impact does that have on the dissemination of personal information?

Mr. DOUGLAS. It is the single biggest impact. It has become the national identifier, although the American people were told it would not be, and I think that is one of the reasons you see cynicism around the country and the concerns with privacy around the country that you talked about in your opening statement this morning when you were back in your district. Because people are aware of this, and they do know that—they are told on the one hand, don't provide that, you don't need to provide that, yet at last count I think 23 of the States in this Nation for the driver's license number use the Social Security number.

So even if you provide your driver's license number, and we have all done this, especially if we live locally, Virginia has it, although again you can opt out of that process, but again how many do; the District uses it, that the clerk will record that on the back of the check.

Many people, such as Ms. Twentyman, who end up as identity theft victims, need to remember there are 400,000 cases a year by the Secret Service's statistics, not some privacy whacko group; the Federal Government, recognizes 400,000 cases a year of identity theft in this country, that begin in just such a fashion, with information that is put down for purposes that is of questionable use. But yet, if you go in there, Mr. Hutchinson, and tell them well, no, I have been taught that I don't need to give that, in many cases they won't complete the transaction with you, even though that is not necessary for the transaction by any stretch of the imagination.

So the Social Security number problem is the most frequent question I get when I talk to people on the Hill, and it is a very complex one, because it is so ingrained in so many systems around the country, and because it has become the default national identifier to tomorrow, say, well, for Congress to outlaw it, that somehow tomorrow it would crash the economy of this country.

Mr. HUTCHINSON. You are saying that if we outlawed the use of Social Security numbers beyond the original intent, which is I guess you give it to your employer so that you can make sure you get credit for your FICA taxes that are paid.

Mr. DOUGLAS. Correct.

Mr. HUTCHINSON. If we outlawed it beyond that limited use, what impact would that have?

Mr. DOUGLAS. I am sure you would hear loud and clear from the business communities that so many are using that as the national identifier, how will they now identify individual transactions that go through. That has become the national identifier. Every business in America that keeps information on our citizens and, you know, very valid reasons, whether it be medical records, financial

records, the things that make our economy hum, to identify us use the Social Security number.

Mr. HUTCHINSON. There is benefit to consumers for that as well.

Mr. DOUGLAS. Absolutely. That is one thing, and I touch on it a little bit more in my full statement. We need to be very careful, and that is why I wholly support this approach that is presented here today, because the piecemeal approach of legislation could be very dangerous.

I think there needs to be—we need to take a deep breath. Gramm-Leach-Bliley just passed, the DPPA is just starting to kick in; I am not as familiar with the medical area, but it is just starting to kick in. We need to step back and take this 18-month look at, first of all, how do some of those provisions that are out there kick in, what effects do they have, and to find a comprehensive way to deal with that. Because to just take a rash approach tomorrow because of concerns I think would have a serious impact on the business community.

Mr. HUTCHINSON. Thank you. Do I have any time left, or is it gone?

Mr. HORN. Sure.

Mr. DOUGLAS. My fault. I am so long-winded.

Mr. HUTCHINSON. Let me just ask one more question if I might which follows up on that.

Dr. Appelbaum, you mentioned that one thing the commission could do is to increase public awareness. If you would just sort of elaborate on that a little bit, particularly in the area of medical records. We have a limited amount of protection now, but there are some things that consumers can do to protect to a greater extent their own information; is that correct?

Mr. APPELBAUM. There is, yes. There are a number of such steps that they can take, of which most people are unaware. An increasing number of States, for example, give patients the right to access their own medical records and to make corrections to those records if errors are found, before the records are widely disseminated, potentially, to their disadvantage. Most people don't know that. There are institutions such as the Medical Information Bureau in my home State of Massachusetts which collects medical-related information for the insurance industry, and similarly will allow individuals to find out, not easily, but to find out the information that is being kept in their files, and correct it, and most people are unaware of that as well.

Mr. HUTCHINSON. Let me interrupt, because I want to yield back my time, but the commission I think is important, that if you conduct hearings across the country, you engage in getting information of the problems that are out there, but also educating the public as to things that they can do themselves to protect privacy, and I think that is very important.

Mr. Chairman, thank you for your leniency, and I yield back.

Mr. HORN. I thank the gentleman and I now yield to the ranking member, Mr. Turner, the gentleman from Texas.

Mr. TURNER. Thank you, Mr. Chairman.

Ms. Twentyman, I want to thank you for your testimony. It has been very enlightening to understand what you have gone through. I notice you mentioned in one part of your testimony that you had

$13,000, I believe it was, in one credit card account alone that was taken?

Ms. TWENTYMAN. Just in 3 or 4 days.

Mr. TURNER. In 3 or 4 days.

Ms. TWENTYMAN. Right.

Mr. TURNER. You mentioned, I think, later in your testimony that you haven't personally been held accountable for any of these balances. These credit card companies, do they have some kind of protection for you as a credit card holder that ensures that you don't have to pay when somebody steals from your credit card account?

Ms. TWENTYMAN. I don't know whether it is insurance or what, but all of them have, as soon as I report it, they take it off my account and tell me I am no longer responsible for it. I am not sure with their bookkeeping what they do with that money, but fortunately I haven't had to repay any of it.

Mr. TURNER. Mr. Douglas, have you had any experience with that? Do these credit card companies just routinely insure against theft?

Mr. DOUGLAS. Yes, sir. The consumer is only liable in theory for $50, if they make prompt notification, to the credit card company and most credit card companies will even waive that $50 on behalf of the customer in order to hold on to the customer.

The thing that should be noted on this, although the customer is not losing out, the business is. And they are not necessarily insured, they are self-insured in this area. Current statistics show that on Internet transactions, and only 1 percent currently over the last Christmas season, only 1 percent of purchases were made by the Internet, 25 to 35 percent of credit card transactions currently made on the Internet are fraudulent, and the people picking up the tab on that are the Internet companies. They lose out. They end up biting the bullet on that. So again, if that area is not addressed, it will be a strain on the advance of the Internet economy.

Mr. TURNER. What kind of enforcement ability do we have to control this? It seems to me law enforcement is totally ill-equipped to deal with any of this.

Mr. DOUGLAS. I think currently they are. I think they are scrambling quickly to catch up. I know the Washington Post has documented just within the last week some efforts on behalf of the FBI to get up to speed in some of these areas, but as in many areas of crime, the thieves are often far ahead. It should be noted, an awful lot of that, especially in the Internet transaction area, is occurring overseas where we have no enforcement jurisdiction. So many of the software packages that are being developed for Internet businesses, I-businesses, in order to preclude fraudulent transactions are totally ruling out any transaction from overseas.

Mr. TURNER. When you said 25 percent of the e-commerce transactions are fraudulent, you are talking about purchases?

Mr. DOUGLAS. That is correct.

Mr. TURNER. With use of a credit card?

Mr. DOUGLAS. Right. Somebody claiming to be Mr. Turner to buy a pair of Nikes is not Mr. Turner, but somebody else. We have all seen when you have gone to a Web site and ordered that you can have it delivered to another address. That is what they will do,

they will put in the credit card information and have it delivered to another address, which is often a vacant home or they are in cahoots with somebody else.

Mr. TURNER. What is the source of that 25 percent figure? Who compiles that kind of information?

Mr. DOUGLAS. You will see that in almost any of the Internet commerce magazines that are tracking this information.

Mr. TURNER. What is the track record with regard to theft from bank accounts? Of course I don't mean just Internet banking, but theft from bank accounts of individuals? Do we have any compilation of totals or is that a very common thing?

Mr. DOUGLAS. I don't have any compilations of totals. When you deal with the identity theft that I have talked about, which is pretext, it is very hard to track, because often it is done and the person doesn't know how it is done; just as Ms. Twentyman said, they never have caught the person. So a lot of people don't report, a lot of people are embarrassed about it, and I am sorry to say that our most fragile and under protected citizenry in this country is senior citizens who this happens to quite regularly.

A lot of this is done over the phone. I have talked about methods that are used to get it from the actual institutions, the same methods are used to defraud our citizens by phone, and senior citizens are the most vulnerable because they grew up in a generation that was polite and didn't just hang up the phone on somebody.

Mr. TURNER. Is there any source of compilation of theft from bank accounts using any of these methods, or is this the kind of information banks wouldn't like to talk about too much?

Mr. DOUGLAS. Well, let me give you an example. There was an information broker by the name, a company called Source One, run by one individual by the name of Peter Easton out of New York. The State of Massachusetts has been the most aggressive in this area. They civilly prosecuted, I think, 10 companies, and he was the only one that went to trial, and they found thousands of cases in just his situation alone. Touchtone that I talked about before from Colorado is currently under a proceeding in the FTC and they also, when they saw his records, found thousands of these cases. Docusearch employs 18 people, Touchtone employed 12 or 18 people, and these are just one of hundreds or dozens of companies around the country.

So you could work the statistics backward that way from the few successful prosecutions and know that this is happening thousands of times a day around the country, if that is helpful.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. We thank you. Let me ask just a few questions to the panel. I might say for my colleagues, if you pick out your voting card, which is your identity card, the Social Security number you have is printed on the card. So be careful.

Anyhow, how about the chance to look at H.R. 4049, the Hutchinson-Moran bill. Do you have any suggestions on it? There is the markup of the commission and their purposes and so forth rather well set out. Dr. Appelbaum, do you have any thoughts on it?

Mr. APPELBAUM. Yes, I do, Mr. Horn. The composition of the group is laid out in terms of its bipartisan nature. But I think for the purposes of achieving true privacy protection, it would be im-

portant to build into this legislation some balance among the various actors in this area, since interests are genuinely conflicting and everyone should be represented. The National Committee on Vital and Health Statistics, which is similarly charged to explore this area, has on it, although it was balanced from a partisan perspective, no consumer representatives, no patient representatives, no privacy advocates, and one practicing physician, and it is that kind of imbalance that we would hope would not occur with this new and very promising privacy commission proposal.

Mr. HORN. So you are saying in the appointments by the majority leader, minority leader, Speaker, and President, there ought to be, the kind of person they pick would have some major concern, maybe, on this particular matter. I don't know how the gentleman who authored this feels.

Mr. HUTCHINSON. Well, first of all, I agree completely that this commission should be composed of people that represent a broad range of the stakeholders in this issue, and second, that they are openminded to this issue. But the reason that was not—when we thought about specifically delineating different representatives on it that sure enough we will leave somebody out, for one thing, and the balance of it, and I felt like, and we have talked about this with Congressman Moran, that the political process would work; in other words, these stakeholders are going to be asking and putting pressure on the appointing people to make sure they are represented on it. I am certainly open, if we need, and we can do that fairly, to delineate that, but that was the thinking, anyway.

Mr. HORN. You mentioned, Mr. Douglas, in your testimony about the Colorado case, and you also mentioned what went on in Virginia. Now, what are the penalties the States have? Have you sort of taken a look at those? I want to tell the staff on both sides that the American Law Division will be asked to give us a paper on the penalties. But I wondered what your experience is; just for this hearing.

Mr. DOUGLAS. When it comes to the use of pretext and other means of fraud and deception to gain information, most of the States have nothing specifically on point. In fact, the Federal Government didn't, until the Financial Information Privacy Act under Gramm-Leach-Bliley, and that is specific to a very narrow range of pretext methods used against financial institutions.

As I noted in my written statement, most of the information brokers have figured out, or are either ignoring it or have gone underground, unfortunately, that is quite a few of them, or figured out other techniques that I am aware of to get around it. Gramm-Leach-Bliley's enactment brought the first Federal criminal provisions ranging from 5 to 10 years, depending upon the dollar amount involved, or the size of the company. But most of the States have nothing. There had been really no prosecutions.

There is some argument that Federal or State wire fraud laws might apply. Perhaps the identity theft law that Congress passed a year or two ago might apply, but we have seen relatively few criminal prosecutions at all. In fact, only 1 State criminal prosecution, no Federal criminal prosecutions, and about 12 civil prosecutions under Deceptive Trade Practices Act types of legislation the State mirrored on the FDC's regulations, if that is helpful.

Mr. HORN. Have you had a chance to look at the Secretary of Health and Human Service's temporary regulations in this area and what the penalties are?

Mr. DOUGLAS. I have not.

Mr. HORN. Have you had a chance to, Dr. Appelbaum?

Mr. APPELBAUM. Yes, we have looked at them extensively.

Mr. HORN. Well, if you would like to file a statement for the record, that is fine. We will do it at this point. Because I realize sometimes in a hearing situation you don't have a chance to really see the language and all the rest of it, so we would welcome the thoughts from you, and your colleagues.

Mr. APPELBAUM. We will do that.

Mr. HORN. To all of you I would ask, what is the extent of the problem with the law enforcement agencies and how easy is it to, let's be charitable and say provide incentives to them to give some of this information, which I guess you could also say are bribes. What has been your experience, Mr. Douglas, with these cases?

Mr. DOUGLAS. I am sorry, I misunderstood the question.

Mr. HORN. Well, the question is, when your friendly local law enforcement agency has a lot of information and you, as a private detective, what are your feelings about what your colleagues do and maybe you do to gain information?

Mr. DOUGLAS. I am with you now. The purchase or bribing of information kept in Federal databases, including law enforcement, that area has actually subsided quite a bit with a round of prosecutions that took place around 10 years ago. It was quite common in the private investigative industry to have a friend in law enforcement, or many PIs are ex-law enforcement who would obtain NCIC information, which is arrest and prosecution records maintained in a Federal database. That has really come to a close, because a number of people have been prosecuted for it, so you don't see quite as much of that going on today.

Mr. HORN. How about with insurance companies? Can they be subjected to sort of getting information out of them to people that maybe shouldn't have it?

Mr. DOUGLAS. Absolutely, and their Web sites, I didn't include any in my presentation today, but where I could go and find out what your life insurance policy is valued at; any of your insurance areas. I also didn't include in these charts stocks, bonds, mutual funds. Any position that you can think of, I can tell you a way to get it.

Mr. HORN. Well, we thank you. We have to get to the next panel if we are going to adjourn at 12, so thank you very much. We really appreciate the time you have taken and the wisdom you have provided. I know, Ms. Twentyman, that it is really something like a stalker that is out somewhere.

Our next panel consists of Professor Fred Cate, professor of law and Harry T. Ice faculty fellow at the Indiana University School of Law in Bloomington; Mr. Travis Plunkett, legislative director, Consumer Federation of America; Mr. Ari Schwartz, policy analyst, Center for Democracy and Technology; and Sandra Parker, esquire, director of Government Affairs and Health Policy, Maine Hospital Association.

[Witnesses sworn.]

Mr. HORN. All four, the clerk will note, have accepted the oath.

So we will start with Professor Fred Cate, professor of law and Harry T. Ice faculty fellow at the Indiana University School of Law in Bloomington. Now, they have a school of law also in Indianapolis, don't they?

Mr. CATE. Yes, Mr. Chairman, they do.

Mr. HORN. But is the main one at Bloomington?

Mr. CATE. They would resent the definition of "main" as being in Bloomington; there are two separate law schools.

Mr. HORN. Well, you have a beautiful campus there in Bloomington. I was a fellow there for a week, 30 years ago, and it is impressive, what you are doing at Indiana.

Mr. CATE. Thank you, Mr. Chairman.

Mr. HORN. Please proceed.

STATEMENTS OF PROFESSOR FRED CATE, PROFESSOR OF LAW AND HARRY T. ICE FACULTY FELLOW, INDIANA UNIVERSITY SCHOOL OF LAW, BLOOMINGTON; TRAVIS PLUNKETT, LEGISLATIVE DIRECTOR, CONSUMER FEDERATION OF AMERICA; ARI SCHWARTZ, POLICY ANALYST, CENTER FOR DEMOCRACY AND TECHNOLOGY; AND SANDRA PARKER, ESQUIRE, DIRECTOR OF GOVERNMENT AFFAIRS AND HEALTH POLICY, MAINE HOSPITAL ASSOCIATION

Mr. CATE. Thank you very much.

Mr. HORN. As you know, your statements are in the record; summarize it so we have time for questions.

Mr. CATE. I will do so. Let me say for the record, I specialize in privacy and information law-related issues. I am testifying today not only as somebody who specializes in that area, but also on behalf of the Financial Services Coordinating Council, which, as I believe you know, is an alliance of the principal national trade organizations in each of the financial services sectors that deal with issues that cut across those sectors, including privacy.

I think, as the prior panel showed, and something which I believe all of the members of this committee certainly already knew, the issue of privacy is not only incredibly urgent, it is also enormously complex. It arises in many different contexts, it involves many different types of information, it involves use of information by many different people. As a result, efforts to deal with privacy issues, whether those efforts are regulatory or legislative or technological, are themselves also inevitably quite complex, and there are a great variety of them. It is precisely because of this complexity and variety that the comprehensiveness of the proposal for a privacy study commission is certainly laudable. The idea of bringing together in one place a focus on a wide range of issues is certainly laudable.

Let me be very specific, however, and offer two comments about the proposal itself.

One is the issue of what do you do about financial information? Congress has just in the past year passed the Gramm-Leach-Bliley Financial Services Modernization Act, that has not even yet been implemented, regulations are currently pending, and that bill itself calls for a study to be conducted by the Department of the Treasury. The risk of duplicating that effort or of rewriting one set of

regulations before an existing set even comes into play is a very great one and is something that I think this bill and the Congress in considering this bill will need to deal with explicitly. What is to be done about the fact that this is an area in which we have already recently undergone extensive regulation.

I might also note in relation to the prior panel, financial services is an area that is already subject to considerable regulation. It has Federal regulators, it has State regulators. This is not an area without a framework of law that already exists and it is one that Congress has recently taken considerable steps to strengthen.

The second point that I would like to make is the one which I believe was also made clearly on the last panel and that is really the key need that if there is a privacy study commission—the importance that its charge be broad, that it not be limited only to looking at the urgent need for privacy protection, but also at the cost of privacy protection, at the cost of inappropriate privacy protection, and at the alternatives to using laws or further regulation for privacy protection.

Now, I think that is clearly captured within the pending legislation. I am not in any way suggesting that change to the bill as I read it, but rather highlighting the importance that if this commission is to engage in what Representative Moran called the "thoughtful, deliberative" process, it needs to have that broad charge and to consider the value of information flows, as well as some of the risk posed by those information flows.

Let me stop there and allow for questions later.

[The prepared statement of Mr. Cate follows:]

Subcommittee on Government Management, Information and Technology
Committee on Government Reform
U.S. House of Representatives

THE PRIVACY COMMISSION: AN EXAMINATION OF PRIVACY PROTECTION

Professor Fred H. Cate

on behalf of the

Financial Services Coordinating Council

April 12, 2000

Mr. Chairman and Members of the Subcommittee:

My name is Fred Cate, and I am a Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute at the University of Indiana School of Law—Bloomington. For more than a decade, I have researched, taught, and written about information law issues generally, and information privacy specifically.[1] I am appearing today on behalf of the Financial Services Coordinating Council, for which I recently completed a research report on *Personal Information in Financial Services: The Value of a Balanced Flow.* The FSCC is an alliance of the principal, national trade organizations in each of the financial service sectors, formed to address issues which cut across financial industry lines. Its members are the American Banker's Association, the American Council of Life Insurers, the American Insurance Association, the Investment Company Institute, and the Securities Industry Association. The FSCC is pleased to be able to present its views on H.R. 4049, the Privacy Commission Act.

There is obviously a great deal of consumer concern over privacy issues. That concern touches on many issues—ranging from identity theft, credit card fraud, and other criminal uses of personal information, to complaints about telemarketing calls during the dinner hour, seemingly

[1]A biographical statement is attached. In compliance with House Rule XI, clause 2(g)(4), I certify that I have received no federal grant, contract, or subcontract in the preceding two fiscal years.

endless solicitations from charities, and so-called "cookies" used by websites to track the habits of internet users; many types of information—ranging from sensitive medical information to video rental records; and many users of information—public and private, foreign and domestic, disclosed and undisclosed. In short, there are a wide variety of distinct consumer concerns and contexts involved in the current privacy debate.

However, we wish to highlight two important points that we believe the subcommittee should bear in mind as it considers the constitution and activities of the proposed privacy commission.

Financial Privacy Provisions

First, one important set of privacy issues—those surrounding the use of personal financial information by financial institutions—has recently been subjected to intensive congressional review. Just last November, as part of the Gramm-Leach-Bliley Financial Modernization Act, Congress adopted sweeping new privacy protections for customers of the nation's financial institutions. These new provisions supplement and broaden earlier-enacted privacy provisions—contained in the Fair Credit Reporting Act, the Fair Credit Billing Act, and in state insurance privacy statutes—to subject banks, insurers and securities firms, whether operating individually or as part of diversified financial entities, to the most extensive privacy restrictions ever enacted at the federal level.

In addition, the federal banking and securities regulators, in consultation with state insurance regulators, have proposed expansive regulations to implement the new privacy requirements. These regulations will become final on May 12 of this year. Six months later, on November 12, the full package of statutory requirements and regulations will go into effect.

Briefly, the major provisions of Gramm-Leach-Bliley are as follows:

- Financial institutions must adopt policies on the collection and use of non-public personal financial information and must disclose such policies to their customers at the time the customer relationship is established and at least annually thereafter.

- The notice must specify the types of information collected and the types of entities, whether affiliates of third parties, to which the institution would propose to disclose such information.

- There must be a "clear and conspicuous" notice of the customer's right to "opt-out", or prevent the disclosure of his or her personal financial information to unaffiliated third parties. (To answer criticisms of some previous uses of the opt-out which were deemed to place an unreasonable burden on consumers to be exercised, the regulations also require that this opt-out provision be easy to exercise, as with a pre-addressed card, a click-through screen or a toll-free number.)

- Financial institutions are prohibited from disclosing customer credit card numbers and other account number information to unrelated third parties for marketing purposes.

- Financial institutions are required to initiate procedures to protect the security and confidentiality of their customer's non-public personal information in conformance with the new standards established in the bill.

- Identity theft and obtaining personal information under false pretenses are made federal crimes.

These are not insignificant mandates. As a result of Gramm-Leach-Bliley, financial institutions will bear the most extensive obligations with regard to the privacy of personal, non-public information of any type of business.

The privacy provisions of Gramm-Leach-Bliley provide real protection to consumers, but come at a price. As we are beginning to realize, implementation and compliance with these provisions are going to be complicated and time-consuming and will entail significant costs, not just for those financial institutions that choose to affiliate, but for all of them. Approximately forty thousand financial institutions will be sending as many as two and a half billion notices to their various customers by December 12. Estimates are that individual households will receive an average of twenty notices each. Printing and mailing costs alone will be in the hundreds of millions of dollars, if not more.

These disclosures will just be the tip of the iceberg. The costs of establishing privacy policies, training employees, setting up internal mechanisms to coordinate differing information systems between subsidiaries and segregating the information of those that opt-out will also be high. So will establishing new security systems and systems for monitoring overall compliance with the Act. The more subsidiary operations a company has—and many diversified financial companies have scores of affiliates—the more complex the task will be.

Enforcement by the regulatory agencies will be no less complicated or burdensome. They know they will be operating under the glare of Congress and the public to make sure the intent of the bill is carried out, and this is a huge undertaking for them as well. And it is important to remember that the costs of implementing, complying with, and overseeing these new regulations will be borne by consumers, as well as by business and government.

In order to gauge the effectiveness of these new measures in protecting the financial privacy of consumers, Gramm-Leach-Bliley also requires the Department of the Treasury to conduct a comprehensive study of information-sharing practices among financial institutions and their affiliates and report back to Congress by January 1, 2002.

For this reason, while we do not oppose the creation of a privacy study commission as envisioned by H. R. 4049, we believe that, in the area of financial privacy, it would largely

duplicate the Treasury study Congress directed just six months ago. Even so, we are confident that with the Gramm-Leach-Bliley privacy provisions in force and fully implemented by the financial institutions regulators, the financial services industry would receive an excellent report card. Relatedly, if the Subcommittee determines to move forward with H.R. 4049, we would urge that the bill specifically include financial industry representatives among the commission members, both because of the importance and widespread use of financial information and to take advantage of the considerable experience this industry has developed and is in the process of expanding in implementing federal regulations and self-regulatory measures to enhance consumer privacy.

The Beneficial Uses of Personal Information by Financial Institutions

The second consideration we would urge the Subcommittee to consider when constituting and charging the privacy commission is the critical need for balancing legitimate privacy interests with the responsible, productive use of personal information. The financial services industry has extensive experience with achieving this balance, the need for which was the subject of my report, *Personal Information in Financial Services: The Value of a Balanced Flow*, that the FSCC recently published. The privacy provisions of Gramm-Leach-Bliley were intended to protect the legitimate privacy concerns of consumers while at the same time preserving the benefits to consumers, as well as to businesses and the economy as a whole, that responsible information-sharing produces. In examining the privacy issue, however, it has become all to easy for industry critics to lose sight of the benefits side of the equation.

Most financial institutions recognize that the most valuable resource they hold is public trust. Historically, the focus of the financial services industry's trust relationship with customers has been on the responsible handling of information—protecting against unnecessary disclosure or fraudulent use, ensuring the accuracy and security of that information, and using information productively—so that the customer benefits. Few customers commit their personal information to financial institutions without the expectation of personal benefit: interest on a savings account,

money to buy a house or car, insurance against unanticipated loss, gains in the stock market to provide for a comfortable retirement.

The responsible use of information to serve the needs of customers is the very definition of the trust relationship that financial institutions have such a long history of achieving and it is exactly what most people expect of the financial services industry. It is the balance between respect for personal information and its responsible, productive use that has yielded exceptional benefits for consumers and contributed to the longest sustained economic growth in modern history. Opt-in legislation and limits on affiliate-sharing threaten to destroy that balance, and with it the many benefits that have resulted from responsible information use and the economic prosperity to which that use has contributed.

The importance of information-sharing in the modern American economy cannot be overstated. The rapid and reliable availability of accurate and complete personal information is essential to—it is no exaggeration to say that it is the very foundation of—virtually all financial services. The benefits of responsible information-sharing include:

Improving the Speed, Availability, and Affordability of Credit and Other Financial Services. The almost universal reporting of personal information about consumers is the foundation of consumer financial services in the United States and, in the words of economist Walter Kitchenman, a "secret ingredient of the U.S. economy's resilience." The responsible use of personal information enhances the speed of credit, insurance, and many other financial services decisions; reduces the cost of virtually all financial services; gives consumers real choices; facilitates consumer mobility; and "democratizes" opportunities.

Providing Efficient, Reliable Service. The sharing of personal information is essential to the services that financial institutions provide to their customers. In fact, many transactions performed today by financial institutions require access to customer information across affiliates. For example, debit and credit card transactions, one-stop-shopping, consolidated statements and

customer service, and comparison-shopping for insurance and investments all require standardized, reliable sharing of customer information.

Identifying and Meeting Customer Needs. Information-sharing allows financial institutions to provide their customers with tailored services that recognize and respond to their individual needs. Financial institutions notify customers who maintain high balances in checking accounts of the availability of higher return investments; analyze customer data to protect customers against inappropriately risky investments; offer customers with recurring credit card balances lower-interest home equity loans; provide customers with bundled services at a single lower price; aggregate all of a customer's accounts to satisfy minimum balance requirements; make instant decisions whether to increase credit lines; create new investment and insurance products; and offer co-branded products, such as affinity credit cards. These uses of data allow the institution to provide customers with valuable, targeted opportunities.

Informing Consumers of New Opportunities. Financial institutions use their own information, as well as data from public records and other sources, to inform consumers most likely to be interested in new products and services. Target marketing dramatically reduces the cost of soliciting customers, thereby lowering their costs and improving the likelihood that a customer will in fact be interested in the service or product; reduces the impact on the environment; and allows new and smaller businesses to compete more effectively with well-established competitors.

Preventing and Detecting Fraud. The financial services industry uses personal information to prevent and detect fraud, recognize atypical behavior that may signal unauthorized credit card or debit card use, share information about lost or stolen cards with affiliates, reduce fraudulent insurance applications and claims, recover stolen funds, and deter money laundering.

Ensuring Solvency and Facilitating Safety. Access to customer information helps ensure the solvency of the U.S. financial services industry. That information helps companies

innovate, attract customers with new services and products, control costs, target market, prevent and detect fraud, make better decisions about loans and credit opportunities and avoid delinquencies and bad debts. In short, access to personal information, in the words of Federal Reserve Board Chairman Alan Greenspan, makes individual financial institutions "more creditworthy and efficient," and the U.S. financial services sector "more transparent and stronger in general."

Responsible information-sharing also facilitates compliance with legal obligations. Regulators and auditors use standardized data to identify unusual transactions and accounts, evaluate the risk associated with different portfolios, and compare institutions and portfolios nationwide. Internally, many financial institutions centralize their compliance activities in a central unit, responsible directly to the CEO or President. This helps ensure effective oversight across all affiliates and guarantee the independence of institution officials responsible for compliance.

Improving Efficiency and Lowering Costs. Financial institutions rely on personal information to operate more efficiently and reduce costs to consumers. Affiliated companies can combine their data systems and operations, thereby acquiring information systems more cost-effectively, avoiding the costs of maintaining redundant systems, and employing fewer technicians. Information-sharing also allows financial institutions to outsource many basic business operations, such as customer account servicing, records management, claims administration, auditing, check-printing, and certain compliance functions. Integrated data systems and third-party contractors offer enhanced services, customer convenience, and lower costs.

Serving the Underserved. The many services that financial institutions use information to provide are especially important for middle- and lower-income Americans. The middle class and previously unserved or underserved populations benefit most directly from lower financial services prices, the dramatic expansion of financial services, 24-hour online banking, reduced

transaction costs of stock purchases and other investments, consolidated statements and service centers, universally accepted credit and debit cards, instant credit, and the creation and marketing of new investment products. Market-wide information sharing allows for a vibrant reinsurance market, which permits broader sharing of previously unacceptable risk. As a result, many Americans who were previously thought uninsurable, today can obtain reasonably priced policies. Information-sharing has allowed the financial services industry to deliver benefits to those Americans who need them most.

Promoting Competition and Helping Small Companies. New and smaller financial institutions—such as community banks, independent insurance agents, and Internet brokerage services—use accessible personal information to compete more effectively with larger companies. Target marketing allows companies without extensive customer lists of their own or the resources to engage in mass marketing, to reach customers most likely to be interested in their products or services. The ability to outsource information processing and marketing tasks permits companies to manage data effectively without investing in expensive information systems and personnel. Data-sharing allows new companies to emerge that specialize in single financial services products or services. Similarly, data-sharing is a prerequisite for independent agents and brokers, who offer their clients a wide range of products of services offered by many different companies. Enhanced competition increases opportunities for customers and reduces prices.

Facilitating E-Commerce and Innovation. Responsible information-sharing facilitates innovation in financial services and products and the ways in which they are provided to customers. In addition, one of the largest components of electronic commerce in the United States today is in the field of financial services. Online stock trades, insurance applications, and banking services—effectively all digital financial services—require sharing information.

To provide all of these and other opportunities, access to data is essential. Laws restricting affiliate-sharing or requiring ad hoc opt-in consent make the provision of these

services, and the convenience and benefits they provide, untenable. It is no answer to condition these services and products on consumer consent, because it is impractical and prohibitively expensive to build and operate the systems that compare data in literally millions of accounts on an ad hoc basis. Virtually all of these information uses depend upon the routine availability of standardized, reliable, complete data. Moreover, the sheer cost of seeking consent would act as a dramatic disincentive to investing in innovation.

This does not mean that privacy is unimportant or unprotected, but rather that it must be balanced—as consumers do everyday—with the benefits that flow from the responsible use of personal information. The privacy commission's important work will be better served if the commission is constituted to include members who are knowledgeable about and experienced in not only privacy, but also the value that flows from responsible use of personal information and the costs—to both business and consumers—of overprotecting or inappropriately protecting privacy.

Conclusion

In closing, I want to re-emphasize that the financial services industry is committed to protecting the privacy of customer financial information in full compliance with the requirements of the Gramm-Leach-Bliley Act. The FSCC believes that, in combination with existing privacy requirements under other laws, these new provisions provide financial institution customers with more extensive privacy protections than customers of any other industry. Finally, should the decision be made to move forward with H.R. 4049, we strongly urge the Subcommittee to recognize the need for the proposed privacy commission to take a balanced approach to the issue of information-sharing, cognizant of the recent legislation and ongoing rulemaking proceedings concerning financial information and of the substantial benefits which responsible information-sharing produces.

Thank you.

Mr. HORN. Well, thank you very much, Mr. Cate. We will go to Mr. Plunkett. Mr. Plunkett is the legislative director for the Consumer Federation of America.

Mr. PLUNKETT. Good morning. Thank you very much for the opportunity to offer our comments today, Chairman Horn, and Mr. Turner. We commend the subcommittee for examining this important issue.

We agree with everything we have heard so far on the significance and urgency of further action on privacy protection for Americans. I am going to commend Representative Hutchinson, because we have talked, I have talked with his staff and with him about our concern here. It is not that we don't see a need for action with the commission and on privacy, it is just a question for us of what is the most effective and timely course of action.

I too will focus my comments on financial privacy and on that issue in particular, we believe that a commission may actually be harmful, not because of your desire to look at the issue and address concerns, but because momentum is building right now at the State and the Federal level to take action soon. Our fear is that it will stall if a commission is enacted.

Like it or not, if Congress establishes a commission to examine privacy issues, many will urge, and we have already heard it to some extent this morning, that all major privacy proposals be stuck in a deep freeze for 18 months or more. The commission has an ambitious schedule and they might run a little over while the commission is operating.

We do very much welcome the fact that the sponsors of this bill, Mr. Hutchinson in particular, see a need for further Federal action on privacy, and I commend Mr. Hutchinson for highlighting the need for more comprehensive Federal approaches. The American people clearly want it. The Wall Street Journal surveyed its subscribers about the most serious issue facing America in the 21st century, and the top concern was not the economy, education, or illegal drugs, it was the loss of personal privacy.

On financial privacy, there is a great deal of research about what Americans want, very specific research, including a 1999 survey by AARP, that found that 81 percent of its members oppose the internal sharing of their personal and financial information with affiliates, a key issue I will get to in a minute, and 92 percent oppose companies selling their personal information.

The erosion of privacy, which we are all aware of and grappling with, leads not only to annoyances, and I put phone calls from pushy people at dinnertime in that category, it can be harmful. You have already heard a great deal about identity theft, which I would call the signature crime of the Information Age and the anecdotal evidence you have heard this morning is backed up by research. Law enforcement officials report a sudden sharp increase in identity theft.

Another example regarding financial privacy, how this causes real harm, a bank in California's San Fernando Valley sold 3.7 million credit card numbers to a felon who then allegedly bilked card holders out of more than $45 million in charges worldwide.

I would point out that consumers and businesses suffer when Americans are worried about their personal privacy. This is an

issue that I think is very important to keep in mind. FTC Chairman Pitofsky recently noted that concerns about privacy are a major reason why Americans who do use the Internet don't make purchases. He also noted that consumers who do not use the Internet rank concerns about privacy as their top reason for not going on line.

Now, the continuing gaps in financial privacy protection are particularly serious, and we take really a much different position than the previous speaker on this issue. Under Federal law, even the new Financial Services Modernization Act, the Gramm-Leach-Bliley Act, even our video rental records are better protected than confidential experience and transaction information held by financial institutions, in particular, held by those institutions and shared with their affiliates. Affiliate information-sharing is a very significant issue. We all expect that under the Gramm-Leach-Bliley Act, we are going to see the largest consolidation of the financial services industry in American history. That means that we, in terms of information-sharing and abuses and intrusions, what we have seen is the tip of the iceberg. It is going to happen. Most players in the market are honest, they are honest brokers, but we are going to see more intrusion and we are going to see more abuses.

One of the worst information-sharing abuses on record did not involve the selling of information to outside third parties; it involved an affiliate. This is the NationsBank/NationsSecurities case, which resulted in a total of $7 million in civil penalties. It was an inside affiliate-sharing agreement. NationsBank shared detailed customer information about maturing certificate of deposit holders with a NationsSecurities affiliate, which then switched, urged the CD holders to switch to a risky derivative fund. Many of these customers who did this lost portions of their life savings.

Legislation to improve financial privacy protections has been introduced in at least 20 States and in both Houses of Congress. The bills in Congress are bipartisan, they are bicameral. Senator Shelby and Representative Markey are leading the charge and they have also set up, as many of you know, a Privacy Caucus. Several folks here are members, including Representative Hutchinson. Virtually all of these proposals would provide that information could not be shared with either an affiliate or a third party without informed consent.

Once again, I would dispute what you have just heard. This isn't an issue that hasn't been studied, it isn't an issue that hasn't been debated extensively. It is the unfinished business of the Gramm-Leach-Bliley Act and the fact that so many States are looking at this issue, and several are moving these bills, they are not just introducing bills, and most of these bills deal with the same topic. Affiliate information-sharing shows me that it is a good idea to act soon and not wait for a good deal of time.

I would note, even though I won't talk too much about this, you are going to hear more about this in a minute, that considerable progress has been made in terms of studying, debating various proposals on health privacy and Internet privacy as well. The Department of Health and Human Services, for instance, has received 60,000 comments on proposed health privacy regulations. The FTC has undergone numerous rulemaking proceedings on Internet pri-

vacy and has supervised or actually implemented several surveys as well.

So in closing, let me just say that to his credit, Representative Hutchinson has clearly indicated that he doesn't want to delay progress of important privacy legislation with this commission. Our recommendation, and we have some modest recommendations which I won't go into regarding the language of the bill, but our broad recommendation is that the mandate of the commission be narrowed to address very specific issues in need of greater study.

I think you are going to hear in a minute of issues that could be studied at greater length. We would urge those who do support the bill to make it clear repeatedly and on the record that the intent of the study is not to delay needed legislative action on financial privacy and health privacy and Internet privacy. Thank you.

[The prepared statement of Mr. Plunkett follows:]

Testimony of
Consumer Federation of America, Consumers Union And U.S. PIRG
Before The House Government Reform Committee
Subcommittee on Government Management, Information And Technology
Regarding H.R. 4049
To Establish the Commission For The Comprehensive Study Of Privacy Protection
April 12, 2000

Chairman Horn, Ranking Member Turner and members of the committee, thank you for the opportunity to testify today. My name is Travis Plunkett and I am Legislative Director of the Consumer Federation of America.[1] I offer my comments today on behalf of CFA and two other national consumer organizations, Consumers Union[2] and U.S. PIRG[3].

We commend the subcommittee for examining the important topic of privacy protections and for seeking testimony from a wide variety of organizations on H.R. 4049, Mr. Hutchinson's proposal to create a national privacy commission. There is much work to be done on this issue. The increasing lack of personal privacy is a top concern for Americans. We have urged Congress and Federal agencies to move quickly on a number of fronts to provide Americans with greater privacy protections, especially regarding financial privacy.

However, despite the good intentions of the sponsors of H.R. 4049, we do not think the establishment of a privacy commission is necessary for the development or implementation of meaningful privacy protections. The basic principles for protecting individual privacy—the Fair Information Practices--are well-known. In fact, they are the basis for Federal privacy standards for government entities.[4] Many specific proposals to address financial, medical and Internet privacy concerns have been introduced during the 106th Congress.[5] Like it or not, if Congress establishes a commission to examine privacy issues, many will urge that all existing privacy proposals be stuck in the deep freeze for the eighteen months or more that the commission is operating. In the area of financial privacy, H.R. 4049 could actually prove harmful by stalling the development of a consensus that is now emerging at the state and Federal level that stronger protections are necessary—soon.

Privacy is a Top Concern for Americans

We do welcome the fact that the sponsors of H.R. 4049 see a need for further federal action on privacy. We commend Mr. Hutchinson in particular for highlighting the need for a more comprehensive Federal approach to privacy. The American people clearly want it. Last fall, the *Wall Street Journal* surveyed its subscribers about the most serious issue facing America in the twenty-first century. The top concern was not the economy or education or illegal drugs. It was the "loss of personal privacy." In the area of financial privacy, numerous surveys have documented that consumers value their privacy highly. For example, in 1999 AARP found that 81% of its members opposed the internal sharing of their personal and financial information with affiliates and 92% opposed companies selling their personal information.[6]

In its recently released report on electronic commerce, AARP also found that "an overwhelming majority (93%) believe that any personal information they give during a business transaction should remain the property of the consumer and not be shared with other businesses without the permission of that consumer." Further, AARP found that "A large number of respondents (45%) would not permit businesses to share their financial information with other businesses under ***any circumstances.***"[7] [Emphasis added]

A *Business Week* magazine poll recently found that more than three-quarters of those who shop online (78%) are "very" or "somewhat" concerned that personal information will be used to send them unwanted information. Over half of respondents thought that government should pass laws on how personal information is collected (57%).[8]

Federal Trade Commission Chairman Robert Pitofsky recently noted that public opinion polling shows that concerns about privacy are a major reason why Americans who do use the Internet don't make purchases. He also noted that consumers who do not use the Internet rank concerns about privacy as their top reason for not going online.[9]

In the political arena, concern about privacy crosses ideological and party lines. For example Republicans Richard Shelby and Joe Barton, along with Democrats Ed Markey and Richard Bryan, are leading congressional on financial privacy and have formed a bipartisan, bicameral Congressional Privacy Caucus. They have been joined in their efforts by a ideologically diverse array of organizations and individuals, such as Ralph Nader and Phyllis Schlafly. Media commentators and editorial boards across the country have called for stronger privacy laws, particularly in the areas of financial and health privacy. Among them, columnist William Safire has been outspoken in calling for stronger protections:

Your bank account, your health record, your genetic code, your personal and shopping habits and sexual interests are your own business....We're dealing here with a political sleeper issue. People are getting wise to being secretly examined and manipulated and it rubs them the wrong way.[10]

Evidence of the Erosion of Personal Privacy is Widespread

It is hard to take part in even the most insignificant everyday activity without being reminded of the escalating erosion of our personal privacy. Telemarketers with an intimate knowledge of our buying habits call us when we sit down for dinner. Internet advertisers use sophisticated and often intrusive techniques to track our online activities. Information about our most sensitive personal information, from dates-of-birth to Social Security, credit card, and bank account numbers, is readily obtainable on the Internet—for a price. Most supermarkets now require consumers to use loyalty program cards to get discounts and coupons in order to track purchases and build customer profiles for use in targeted marketing. Banks and other financial institutions increasingly share our sensitive financial information with third parties and affiliates in order to sell us new products, many of which are overpriced and deceptively marketed.

Open a paper these days and you will see how easy access to this kind of personal information is increasingly being used for intrusive, deceptive or fraudulent purposes:

- Law enforcement officials report a sudden, sharp increase in identity theft, in which a person's personal information is stolen for use in obtaining loans, credit cards and other goods. The Social Security Administration reports that it received more than 30,000 complaints about the misuse of Social Security numbers in 1999, more than double the number received in 1998 and three times that received in 1997. The Social Security Administration attributes the rise to the ease with which this information can be collected and distributed on the Internet[11].

- A bank in California's San Fernando Valley sold 3.7 million credit card numbers to a felon, who then allegedly bilked cardholders out of $45.7 million in charges worldwide.

- After investigations were launched by the Federal Trade Commission and two state attorneys general, the Doubleclick Company recently announced that it would halt plans to cross-reference information on consumers' online shopping habits with real names and addresses, allowing them to develop profiles of consumer interests that could be highly intrusive.

- The Federal Trade Commission recently disclosed that some web sites that provide health information about consumers have secretly collected information about individuals, which could include diagnoses, prescribed medicines, HIV status and pregnancy, and shared it with others.

Quick Action Needed on Financial Privacy

The continuing gaps in financial privacy protection are particularly significant. Numerous news reports, lawsuit settlements and complaints have documented that the threat to financial privacy is real. Yet, under federal law, even our video rental records are protected better than the confidential "experience and transaction information" held by financial institutions.

This financial privacy gap can easily be closed, but the recently enacted Financial Services Modernization Act (FSMA) is inadequate to do the job. It allows the continued widespread sharing of information, without even an option for consumers to "opt out" of the sharing of their financial experience and transaction information among affiliated financial institutions, as well as with many non-affiliated third parties. The sweep of the exception allowing continued sharing with non-affiliated third parties is broad. Further, while the provisions of the FSMA include a limited restriction on providing account numbers to non-affiliated third parties, that section is narrow and only restricts the sharing of these account numbers for marketing, but no other, purposes. In addition, the purported disclosure provision of the FSMA (Section 503) is narrowly crafted and does not enhance consumer disclosures concerning the practices of affiliate sharing.

Allowing financial institutions to share information with affiliates is a major intrusion. Privacy invasions are made by both affiliates and third parties. In monetary terms, one of the worst information sharing violations documented so far– the Nationsbank/NationsSecurities case, which resulted in a total of $7 million in civil penalties--was an inside affiliate sharing arrangement, not a third party violation. Nationsbank shared detailed customer information about maturing CD holders with a securities affiliate, which then switched the conservative investors into risky derivative funds.[12] The merger of Citibank and Travelers Insurance provides the first example of the potential for the risky sharing of financial and medical information for marketing or underwriting purposes. Since enactment of the FSMA, many bills at the state and Federal level have been introduced to cover information sharing by affiliates.

Companies also share information with third parties. Most recently, a lawsuit brought in June of 1999 by the Attorney General of Minnesota against US Bank has documented that the nation's largest banks have routinely shared confidential customer "experience and transaction" information with third-party firms for telemarketing and other purposes. The telemarketer doing business with US Bank, Memberworks,[13] had contracts with numerous other banks, as did at least one other competitor, Brand Direct,[14] which has also been the subject of consumer complaints. In the Minnesota settlement agreement with US Bank, the bank agreed to stronger privacy protections than those offered under either HR 10, S. 900 or the final FSMA. In particular, the bank agreed to provide notice of customers' rights to "opt out" of the sharing of information with bank affiliates for purposes of marketing financial products and services.[15] However, the settlement agreement also included an "out" clause, which allows the bank to re-open the settlement if Congress passed a weaker law, such as the FMSA.[16]

It should be noted that many of the same financial institutions that refuse to support laws that restrict information sharing among affiliates have agreed to these restrictions in other parts of the world. The U.S. Department of Commerce is close to negotiating a so-called "safe harbor" with the European Commission that will govern the activities of U.S. firms doing business in Europe. The current draft of the safe harbor, while improved over earlier proposals, remains inadequate in our view since it fails to meet the privacy provisions of the 1995 European Data Directive. Nevertheless, it is significant that US firms have agreed to grant their European customers greater privacy protections than their American customers.[17]

Consumer groups do not seek a ban on information sharing, nor would providing informed consumer consent defeat the purposes of financial modernization. We only seek only to give consumers control over the use of their confidential customer information for secondary purposes. Sharing of information for compliance with other laws, or for completing transactions associated with a consumer's existing accounts, is acceptable and possible under proposals offered to improve privacy protection under the FSMA, such as legislation offered by Representatives Markey and Barton, HR 3320 and an identical Senate proposal, S. 1903 , from Senators Shelby and Bryan.

After the House passed HR 10, the House Banking Committee held a hearing on financial privacy. Significantly, the Comptroller of the Currency and the Undersecretary for Domestic Finance both called for stronger privacy protection and, in particular, urged protection of information to be shared with either affiliates or third parties. Although the administration testimony discusses an opt-out, instead of our preferred opt-in, Undersecretary Gensler's testimony is quite clear: "The Administration believes that consumers should have the choice to opt out of -- that is, say "no" to -- the use of their data by both third parties and affiliates."[18]

Then, in conference, FSMA was amended by the so-called Sarbanes amendment, which reversed the recent trend of the Congress to preempt stronger state laws. In a clear statement of Congressional intent, FSMA's Section 507 affirmatively and expressly urged the states to take stronger actions to protect financial privacy. Legislation to improve privacy protections under FSMA has been introduced in at least 20 states. Most state proposals would provide that information could not be shared with either an affiliate or a third party without informed consent. This week, for example, the San Francisco Chronicle editorialized in favor of several stronger bills, including AB 1707, (Kuehl), which passed committee on a 10-5 vote on 28 March 200.

If such legislation were to pass, the companies would, in effect, be forced to sell you on the benefits of giving up your privacy. This would make them more likely to disclose how they are

using the information, and less likely to share it in exploitive ways. Most important: You would be in control. You could determine which types of information, if any, could be shared among affiliates or sold to other companies.[19]

The Need for Comprehensive Privacy Protection

While it is true that the U.S. has relied on a sector-by-sector approach to privacy, rather than an over-arching privacy law, it is emphatically not true that voluntary self-regulation has worked. Although industry groups have succeeded in defeating attempts to enact an overarching privacy law, stronger laws protect consumers in several sectors, including telecommunications, video records, cable television and credit reports. For example, in June of 1999, the local telephone company, Bell Atlantic, sent the following "opt-in" notice to its customers:

> "We understand that privacy is very important to all our customers. So unless we have your permission, Bell Atlantic does not share information about your account – not even with our affiliates – such as Bell Atlantic Mobile and Bell Atlantic Internet."

Unfortunately, strong laws do not yet apply to either financial or medical records, arguablly the most private of records. Further, changes in the marketplace are causing the convergence of sectors. As privacy expert Marc Rotenberg has noted, it is time to consider such an over-arching privacy law:

> Those who argue that the United States has typically protected privacy by self-regulation and industry codes know very little about the long tradition of privacy legislation in this country. It is, however, correct to say that the United States, over the last twenty years, has taken a sectoral approach as opposed to an omnibus approach to privacy protection in the private sector. But it is also important to note that the sectoral approach has several weaknesses. For example, we have federal privacy laws for video records but not for medical records. There are federal privacy laws for cable subscriber records but not for insurance records. I think the problems with the sectoral approach will become increasingly apparent as commerce on the Internet grows. The Internet offers the ideal environment to establish uniform standards to protect personal privacy. For the vast majority of transactions, simple, predictable uniform rules offer enormous benefits to consumers and businesses. It is also becoming increasingly clear that the large industry mergers in the telecommunications and financial services sectors have made the sectoral approach increasingly obsolete. Firms now obtain information about individuals from many different sources. There is a clear need to update and move beyond the sectoral approach.[20]

The notion offered by Internet companies, U.S. banks and direct marketers that voluntary self-regulation either works, or is sufficient to guarantee privacy, is not only unfounded but also "out of step with the rest of the world," according to a recent international study of privacy laws.[21] Consumers should be given a level of privacy protection, based on Fair Information Practices[22], that:

- Gives consumers the right to opt-in for all information sharing for secondary purposes, whether to affiliates or to third parties.[23]
- Gives consumers clear notice and full disclosure of a privacy policies for both affiliate and third party sharing and of the consumer's right to choose.

- Gives consumers full access to all of their records and a right to dispute and correct errors.
- Provides consumers with enforceable legal rights against violators.

Beyond the convergence of commerce on the Internet, mergers and consolidations also pose serious privacy threats that deserve prompt attention. For example, while some have rightfully raised antitrust concerns regarding the AOL-Time Warner merger, our organizations, and others in Europe and the U.S., acting together as the Trans Atlantic Consumer Dialogue (TACD), have also raised privacy concerns:

> ...The combined databases of the two firms would likely produce the most detailed records on consumers ever assembled, from favorite television programs to book purchases to associations with religious organizations and even political preferences. According to the *Wall Street Journal*, "AOL already has the names, addresses, and credit card numbers of its 22 million members. It also has tons of tidbits on ages, interests, and musical tastes of the people who fill out member profile pages or register with AOL's ICQ chat or its Spinner online radio divisions." *The Wall Street Journal* also reports that "Time Warner has the names, addresses and information on the reading and listening habits of the 65 million households who receive its magazines, CDs and books." And USA Today notes that "Time Warner has access to information about its 13 million cable subscribers and from its other businesses, such as *Time*, *Sports Illustrated* and *People* magazines."
>
> Industry analysts predict that "AOL Time Warner will be able to track which television show a person is watching on Time Warner's cable system, as well as the Web sites they surf on AOL. A person watching a health program on a Time Warner cable channel who then visits a site, such as the drkoop.com Inc. page on AOL, could be tagged as someone concerned about health issues - a prime target for ads from pharmaceuticals companies.

Given the risk to consumer privacy that the AOL-Time Warner merger presents, the other mergers between multimedia companies that will likely follow, and the absence of effective measures to safeguard consumer interests, the TACD will urge U.S. officials to condition approval of the proposed merger on the adoption of enforceable Fair Information Practices that would guarantee consumer privacy safeguards at least equal to those that would be provided under the EU Data Directive.

TACD will also urge US officials to pursue adoption of a comprehensive privacy law, comparable to the EU Data Directive, as opposed to the sector specific laws that do not correspond to the range of activities pursued by combined entities such as the proposed AOL-Time Warner corporation..."[24]

A Privacy Commission is Not Needed on Major Privacy Issues; Congressional Action Is

Representative Hutchinson has acknowledged the lack of uniform privacy protections in proposing the Commission for the Comprehensive Study of Privacy Protections. The commission would be charged with examining a broad array of issues related to governmental and private intrusions into personal privacy. It would be required to offer legislative and non-legislative recommendations, as well as cost analyses, within 18 months. The commission would be required to seek input from interested parties and the public at 20 hearings across the country.

Our organizations see a number of problems with the creation of a national privacy commission:

- **Unless the mandate of the commission is narrowed to exclude financial privacy issues, the creation of a commission would delay efforts to put meaningful financial privacy protections on the books**. Enactment of the FSMA is likely to lead to the largest consolidation of the financial services sector in American history. Without adequate protections, Americans' financial privacy will be invaded on an unprecedented scale. Legislation to address the privacy shortcomings of the FSMA has been introduced in more than twenty states and by a bipartisan group of legislators in Congress.[25] Virtually all of these proposals address the fact that banks and other financial services companies can share personal information with their affiliates and many third parties on a vast scale and there is nothing consumers' can do to prevent it. The creation of a privacy commission will delay action on the consensus that is emerging in this legislation. Opponents of further protections have already said that no further action is necessary. They are now touting the possible creation of a privacy commission as another, and very credible, reason for delay.

- **The principles and proposals for meaningful privacy protection already exist**. What is needed is Congressional consideration of the many proposals that have been offered, and then, action. As mentioned above, the building blocks of meaningful privacy protection exist in the form of the Fair Information Practices. Additionally, much groundwork has already been done in the areas of financial and health privacy, through legislative hearings and agency rulemaking. The Department of Health and Human Services have received over 60,000 comments in its proceeding to establish uniform Federal standards for health privacy.

  Congress could move this year to apply the Fair Information Practices to issues surrounding financial, Internet and health privacy and enact legislation. It would be cumbersome legislatively (given the defined jurisdictions of House and Senate committees), but Congress could also develop the kind of comprehensive privacy policy that Representative Hutchinson has suggested might be needed and that consumer groups would support. A significant model for a broad privacy law already exists: the European Data Directive.

- **The questions on privacy that need to be resolved are fundamentally political, not substantive**. As we've seen in the last few years on the issues of Medicare Reform and Social Security, the issuance of a report by a bipartisan national commission on a subject of some controversy is no guarantee that a real consensus will develop in Congress. In 1977, the Privacy Protection Study Commission made a number of recommendations regarding, among other things, financial and medical privacy, that have not been enacted. On Internet privacy, the Federal Trade Commission has been "studying" the issue for quite some time.

  Moreover, if the commission can't finalize a report within 18 months--a real possibility given the breadth of the task and the number of field hearings that are called for in the legislation—it could take up to two more years before the process of putting further protections on the book may begin. After the commission reports, Congress will need to hold hearings, consult with interested parties and the public, mark up proposals and debate them on the Floor. That process should begin now, not in 18 months or two years.

  After the commission issues its report, Congress will still have to grapple with the tough issues surrounding privacy. No amount of study will make issues, such as the following, easier to resolve in a year and one-half than they are now:

- Comprehensive privacy laws versus an uneven sector-by-sector approach;
- Industry self-regulation on the Internet, which in our opinion is harmful to both consumers and the growth of electronic commerce, versus the establishment of reasonable privacy standards;
- Privacy laws based on Fair Information Practices versus continuing to allow businesses to share information for secondary purposes (to affiliates and many third parties) without consumer consent.

Recommendations on the Provisions of H.R. 4049

If subcommitee members decide to support this bill in spite of our concerns, we do have a few specific recommendations on the provisions of the bill. First, we suggest that the commission be required to provide an analysis of privacy protection laws enacted by other countries. This is especially important in light of the in light of the fact that the sharing of information and data knows no boundaries, especially on the Internet.

Secondly, one of the "findings" under Section Two of the bill is very misleading. Finding 10 selectively reports on the results of the Federal Trade Commission's 1999 "sweep" of Internet privacy. All of the surveys of Internet privacy show the same trend: more sites are posting privacy policies but very few of these policies actually provide consumers with real protection, such as the ability to prohibit information sharing. For example, the 1999 Georgetown Internet Privacy Survey found that fewer than 10 percent of the sample Web sites met the minimal information practice standards supported by the FTC, professed by industry self-regulation proponents and expected by consumers (based, once again, on the Fair Information Practices). By reporting only half of this trend, finding 10 leads to the misperception that privacy protection on the Internet is increasing, when, in fact, it is not. We suggest that this finding be amended to note that the FTC also found that very few sites complying with all of the Fair Information Practices in providing adequate privacy protection.

Conclusion

In spite of our serious reservations with the approach proposed in this legislation, we would like to commend Representative Hutchinson and his cosponsors for highlighting the need for further Federal action on privacy and for their serious and sincere efforts to address Americans' growing concern about the serious erosion of their personal privacy. Representative Hutchinson has been forthright in reaching out to our organizations and many others for input on this bill, and we look forward to working with him and the members of this subcommittee in providing greater privacy protection for all Americans.

ENDNOTES:

---

[1] CFA is a non-profit association of 260 state and local affiliates representing consumer, senior citizen, low-income, labor, farm, public power and cooperative organizations. CFA was founded in 1968 to advance the consumer interest through advocacy and education.

[2] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about good, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of Consumer Reports, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, Consumer Reports with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and

regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

[3] U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups. PIRGs are non-profit, non-partisan consumer and environmental advocacy groups active around the country.

[4] 1974 Privacy Act.

[5] Worthy of Congressional attention, although not necessarily endorsed by each of our organizations, are: S. 2328 (Feinstein) and H.R. 1450 (Kleczka) regarding identity theft; H.R. 1057 (Markey) and H.R. 1941 (Condit) regarding health privacy; S. 2063/H.R. 3770 (Torricelli/Jackson) regarding Internet privacy, and H.R. 3307 (Chabot), requiring a "privacy impact statement" for proposed federal rules.

[6] AARP Data Digest #39, Spring 1999, based on national telephone survey. AARP also commissioned a survey of all consumers, which found that only 14% of Americans "completely trust" their credit card companies to protect information about them. 17 Mar 99, AARP Poll: Nearly One In Five Americans Report They've Been Victimized By Fraud <http://www.aarp.org/press/1999/nr031799a.html>

[7] AARP News Release, 30 Mar 2000, "AARP Survey: Many Americans Face E-Commerce Skills Gap," accompanying new survey of 1,000 computer users aged 45 and older.

[8] Business Week/ Harris Interactive Poll of 1,014 people; March 20, 2000.

[9] Speech at the Woodrow Wilson Center; February 10, 2000. Chairman Pitofsky was referring to the IBM-Harris Multi-National Consumer Privacy Survey (1999) and a Business Week/Harris Poll; March 16, 1998.

[10] New York Times, September 23, 1999.

[11] Several bills have been introduced in the 106th Congress that would reduce the incidence of identity theft See for example, HR 1450 (Kleczka) "Personal Information Privacy Act of 1999" and S. 2328 (Feinstein, Kyl, Grassley) "Identity Theft Prevention Act of 2000." Among other purposes, these bills would both shut a loophole in the Fair Credit Reporting Act that allows the sale of detailed demographic information called a "credit header," that includes names, addresses, social security numbers and even mother's maiden names, derived from credit reports.

[12] See SEC Release No. 7532 And Release No. 39947, May 4, 1998, ADMINISTRATIVE PROCEEDING AGAINST NATIONSBANK, NA AND NATIONSSECURITIES, File No. 3- 9596, In The Matter Of : ORDER INSTITUTING CEASE-AND- DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTIONS:15(B)(4) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934 AND FINDINGS AND ORDER OF THE COMMISSION. See < http://www.sec.gov/enforce/adminact/337532.txt> (Note, total civil penalties of nearly $7 million includes fines paid to other state and federal agencies, as well as to the SEC.) From the order:
"NationsBank assisted registered representatives in the sale of the Term Trusts by giving the representatives maturing CD lists. This provided the registered representatives with lists of likely prospective clients. Registered representatives also received other NationsBank customer information, such as financial statements and account balances. These NationsBank customers, many of whom had never invested in anything other than CDs, were often not informed by their NationsSecurities registered representatives of the risks of the Term Trusts that were being recommended to them. Some of the investors were told that the Term Trusts were as safe as CDs but better because they paid more. Registered representatives also received incentives for their sale of the Term Trusts."

[13] On Friday, 16 July 1999, the Minnesota Attorney General filed suit against Memberworks. At least four other states (Florida, California, Washington and Illinois) are investigating the firm. See The Washington Post,. "Telemarketer Deals Challenged in Suit, Sale of Consumer Financial Data Assailed," by Robert O'Harrow Jr, Saturday, July 17, 1999; Page E01.

[14] For articles on BrandDirect and Chase Manhattan, see for example, The Seattle Post-Intelligencer, "You may be a loser -- buying something you didn't want", by Jane Hadley, Thursday, April 8, 1999 or Newsday, " Company Had Her Number / Woman discovers to her surprise card issuer gave out account data" by Henry Gilgoff, 9 May 1999.

[15] Joint press release of Minnesota Attorney General and US Bank, 1 July 1999, <http://www.ag.state.mn.us/home/files/news/pr_usbank_07011999.html >

[16] See Court File 99-872, Final Judgement and Order, Hatch v US Bank, f/k/a First Bank, et al <http://www.ag.state.mn.us/home/files/news/us_bank_judgement.html>: 24. Notwithstanding anything to the contrary in this Order, certain provisions contained in this Order may be modified according to the terms set forth in this paragraph: ... (D) In the event new federal legislation or regulation applicable to national banks and respecting the specific subject matter of any paragraph herein is passed or adopted, Defendants may provide written notice to the Minnesota Attorney General's Office that they believe that such new federal legislation or regulation should result in a modification of this Order.

[17] See 30 Mar 2000 comments of the Trans Atlantic Consumer Dialogue at http://www.tacd.org/press_releases/state300300.html. For more information, go to the US Department of Commerce International Trade Administration http://www.ita.doc.gov/.

[18] See testimony of Treasury Under Secretary Gary Gensler before the Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services, United States House of Representatives, 21 July 1999 <http://www.house.gov/banking/72199gen.htm>

[19] Editorial, "Defending Your Privacy: Speak Now, or Else" page A28, San Francisco Chronicle, 10 April 2000.

[20] Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives May 7, 1998 <http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>

[21] See Global Internet Liberty Campaign, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice." October 1998, <http://www.gilc.org/privacy/survey/>

[22] As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices. Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. <http://www.privacyrights.org/AR/fairinfo.html > The document cites the version of FIPs in the original HEW guidelines, as well as other versions: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973 [From The Law of Privacy in a Nutshell by Robert Ellis Smith, Privacy Journal, 1993, pp. 50-51.]

1.Collection limitation. There must be no personal data record keeping systems whose very existence is secret.

2.Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.

3.Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4.Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

5.Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

[23] This opt-in right is in S. 1903/ H.R. 3320. The bills apply to financial institutions. The opt-in is very clear, prohibiting disclosure of nonpublic personal information unless the consumer "has affirmatively consented in accordance with such rule to the transfer of such information."

[24] See Recommendations of the Trans Atlantic Consumer Dialogue's February 2000 meeting in Washington, DC <http://www.tacd.org/ecommercef.html#aolmerge> on the AOL-Time Warner merger.

[25] S. 1903, introduced by Senators Shelby, Bryan. H.R. 3320, introduced by Members of Congress Markey, Barton, et al.

Mr. HORN. Thank you. We now have Mr. Ari Schwartz, policy analyst for the Center for Democracy and Technology. You might tell us a little bit about that institution.

Mr. SCHWARTZ. Sure. Thank you, Chairman Horn and members of the panel. Thank you for inviting me to testify on the Privacy Commission Act.

CDT believes that the focused privacy commission could help build privacy protections, but as Representative Hutchinson mentioned earlier, it should not be used to derail the current process on important legislative proposals already in front of Congress.

Before going into detail about how such a commission might work, I would first like to explain CDT's view of the current state of consumer privacy. As some of you know, the Center for Democracy and Technology is committed to protecting privacy on the Internet. Recent studies have shown that individuals are growing more concerned about their loss of privacy, both on and off line.

These growing concerns are well-founded. Stories of privacy invasions and security gaps in both the private and public sector are becoming almost daily occurrences. CDT believes that work in three areas, three legs of a stool if you will, are needed to help reverse this trend and build privacy protections for the future.

First, CDT is working with many responsible companies, privacy experts and technologists on privacy-enhancing technologies which are necessary to build privacy into the infrastructure of communications technology such as the Internet and reverse the trend that we have been seeing so much of with privacy-invasive technologies. For example, we are working on a standard with the World Wide Web Consortium called the Platform for Privacy Preferences, or "P3P", which would make privacy notices easier to read.

Many companies are beginning to build P3P into their Internet products. For example, last week Microsoft announced that it has plans to implement P3P in its upcoming consumer software products. Self-regulatory efforts by industry are also important to ensure enforcement on the Internet. As the economy becomes more global and decentralized, responsible practices become an increasingly important tool.

Last, we believe that there is a role for Congress. Legislative approaches are needed. Without the means to imbed fair, predictable results, better encourage self-regulation, or go after bad actors in law, CDT fears that the actions of a single company could cause the public to question the motives of an entire industry. For the reasons that we have heard today, this is especially important in the financial, health and Internet areas.

Congress must move forward in these areas in particular.

A commission such as the one proposed could help learn how to protect privacy. In fact, over the past 30 years, we have seen various kinds of commissions at the U.S. Federal level. I have detailed those in my written testimony in the appendix. However, while the theoretical work of these commissions and panels have pushed privacy forward worldwide, the U.S. consumers have very little to show for it. Therefore, we urge you not to duplicate the work of those past committees and panels, but to move forward and focus the panel on issues that have not been studied.

Some of the areas of special interest to this subcommittee may be: revising the Privacy Act of 1974. As early as 1977, a congressional commission found that the Privacy Act, which protects personal information within the Federal Government, was not as effective as it should be. The act should be examined again and recommendations should be made in light of the advent of government's use of the Internet and the spread of the Social Security number which we have already heard a little bit about today.

Public records such as driver's license information and court records and other information that Mr. Douglas brought forward would also be a useful area to study. We need to reexamine how the government information is made available to the public. The claim that a government document is hard to find can no longer be used as an excuse to keep personally identifiable information available to anyone to sell or use as they wish.

Similarly, government at all levels should be encouraged to post more public information to the Internet. With jurisdiction over both the Freedom of Information Act and the Privacy Act, the two great government accountability and openness acts of the past century, this discussion should be of great interest to this subcommittee in particular.

On access and security issues, the commission could help Congress use the findings of the FTC advisory committee which is just finishing its work on these subjects.

Last, a commission could examine the effectiveness of an individual's private right of action under privacy laws. While the private right of action should remain an integral part of privacy laws, we have seen time and time again that when this is the only option for Americans, they receive no redress. Again, this concern is most clear in the application of the Privacy Act of 1974.

Creating a commission focused on these areas would allow its members to build on the work done in the past. While focusing the commission would better help use taxpayer dollars and allow us to further learn about privacy, the most vital concern facing the creation of a new congressional commission is a political one, as we have heard from Mr. Plunkett and Mr. Hutchinson. The commission must not be used to delay or deter from the discussion or progress of medical, financial or Internet bills that have already been mapped or studies.

I thank you again for having me and look forward to your questions.

[The prepared statement of Mr. Schwartz follows:]

Testimony Of
Ari Schwartz
Policy Analyst
The Center for Democracy and Technology

Before

The House Committee on Government Reform
Subcommittee On Government Management, Information and Technology
April 12, 2000

HR 4049
Privacy Commission Act

Overview

Mr. Chairman and Members of the Committee, the Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about privacy in the online environment and HR 4049, a bill to establish the Commission for the Comprehensive Study of Privacy Protection. CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies. We thank the Chairman for the opportunity to participate in this hearing and look forward to working with the Committee to develop policies that support civil liberties and a vibrant Internet.

I hope to offer the Committee CDT's view on the importance of privacy; what can be done to protect it; and, specifically, what this Committee can do to help. I will attempt to outline three major points:

1) **Privacy is a key concern for the future.** The digital economy has created new threats to privacy. Americans are openly concerned about these threats.
2) **Multiple approaches are needed to protect privacy.** Self-regulation, new privacy-enhancing technologies, and baseline legislation must all play a role if privacy is to be protected in the future.
3) **A commission to study privacy could help, but must not be used as an excuse to delay.** For 30 years, federal commissions have played an active role in shaping privacy in America. We must neither duplicate past work, nor allow a commission to prevent legislation on issues examined by previous commissions from moving forward. This is particularly important in the areas of Internet, medical and financial privacy.

Privacy is a key concern for the future.

I would like to first address privacy, people's expectations of privacy, and the ways in which the evolution of the Internet may threaten personal privacy. As many of you know, the Center for Democracy & Technology has long been an advocate for protecting privacy on the Internet.

CDT believes that a starting point for thinking about privacy online should be individuals' long-held expectations of autonomy, fairness, and confidentiality. By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified. Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. In terms of confidentiality, we need to continue to ensure strong protection for e-mail and other electronic communications. Policy efforts should ensure that those expectations are respected online as well as offline. These expectations exist in both the public and the private sectors.

As it evolves, the Internet poses both challenges to and opportunities for protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints could reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy.

Recent surveys confirm that more Americans are alarmed by the growing threats to privacy. For example, a March 10, 2000 *Business Week Poll*[1] shows that 41% of those online are very concerned about the use of their personal data. This was up from 31% in the same magazine's 1998 study.[2] More telling are the 63% of those who have been online, who have not shopped online, but are very concerned about personal privacy. A September 1999 *Wall Street Journal* Poll indicated that privacy is the top concern of Americans for the next century. A *Wired* Magazine survey in the latest issue showed that when American adults are asked what they like least about the Internet they respond that privacy is the number one issue, three times greater than that of any other concern.

These concerns are not unfounded. Almost every day, another privacy concern or security violation surfaces in the news. In the past two months alone we have seen privacy problems at such well-known companies as DoubleClick,[3] H&R Block,[4] Intuit,[5] and TWA[6] along with countless others. We will not be able to realize the promise of the Internet to promote e-commerce growth sand social interaction online if people cannot protect their privacy.

Multiple approaches are needed to protect privacy.

---

[1] Green, Heather; Mike France and Marcia Stepanek and Amy Borrus. *Business Week.* March 20, 2000. http://www.businessweek.com/2000/00_12/b3673006.htm

[2] Green, Heather with Catherine Yang and Paul C. Judge. A Little Net Privacy, Please. *Business Week.* March 16, 1998 http://www.businessweek.com/1998/11/b3569104.htm

[3] Schwartz, John. "Web Firm Halts Profiling Plan: CEO Admits Mistake in Face of Probes, Privacy Complaints." *Washington Post.* March 3. 1999. A1.

[4] Macavinta, Courtney. "Breach exposes H&R Block customers' tax records." *CNet News.com.* February 15, 2000. http://news.cnet.com/news/0-1005-200-1550948.html?tag=st.ne.1002.

[5] Junnarkar, Sandeep. "Intuit plugs leaks to DoubleClick." *CNet News.com.* March 2, 2000 http://news.cnet.com/news/0-1007-200-1562341.html?tag=st.cn.1.

[6] Konrad, Rachel. Airline's mistake exposes email addresses. *CNet News.com.*. March 21, 2000 http://news.cnet.com/news/0-1007-200-1580221.html?tag=st.cn.1.

Protecting privacy on the Internet requires a multi-pronged approach that involves industry self-regulation, technology, and legislation.

1) Industry Self Regulation
Consumers and Congress must continue to press the Internet industry to adopt privacy policies and practices such as notice, consent mechanisms, and auditing and self-enforcement infrastructures. We must realize that the Internet is global and decentralized, and thus relying on legislation and governmental oversight alone simply will not assure privacy. Because of extensive public concern about privacy on the Internet, the Internet is acting as a driver for self-regulation, both online and offline. Businesses are revising and adopting company-wide practices when writing a privacy policy for the Internet. Efforts that continue this greater internal focus on privacy must be encouraged.

2) Privacy Enhancing Technologies
On the technology front, while the Internet presents new threats to privacy, the move to the Internet also presents new opportunities for enhancing privacy. Just as the Internet has given individuals greater ability to speak and publish, it also has the potential to give individuals greater control over their personal information. For example, the World Wide Web Consortium's Platform for Privacy Preferences ("P3P") will enable individuals to more easily read privacy policies of companies on the Web, and could help to facilitate choice and consent negotiations between individuals and Web operators. Many companies are now embracing this technology, and Microsoft announced last week that it will implement P3P in upcoming consumer technologies.[7] We must continue to promote the development of privacy-enhancing and empowering technology.

3) Baseline Legislation
Finally, CDT believes that we must adopt some form of legislation that incorporates into law Fair Information Practices -- long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."[8] Legislation is necessary to guarantee a baseline of privacy on the Internet, but it is not one-size-fits-all or reactive legislation. As a starting point, privacy legislation is urgent in key sectors such as privacy of medical and financial records. For broader consumer privacy, there needs to be baseline standards and fair information practices to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies. Finally, there is no way other than legislation to raise the standards for government access to citizens' personal information increasingly stored across the Internet, ensuring that the 4th Amendment continues to protect Americans in the digital age.

A commission to study privacy could help, but must not be used as an excuse to delay.

---

[7] Meland, Marius. "Microsoft, AOL Become Privacy Gatekeepers." *Forbes.com.* April, 7, 2000. http://biz.yahoo.com/fo/000407/mu2547.html

[8] Alan Westin. Privacy and Freedom (New York: Atheneum, 1967) 7. See the appendix of this testimony for a listing of Fair Information Practice Principles and how they have developed over time.

A Congressional commission could be an excellent starting point for thoughtful Congressional action on complex consumer and government privacy issues. But it is essential that Congress not allow a commission to slow progress in other areas.

Congressionally appointed privacy commissions of the sort contemplated in HR 4049 could help in each of these three areas. In fact, over the last 30 years, dozens of federal government commissions, workshops and advisory boards have put together some of the most complete and important work on privacy. However, while these federal commissions have provided some of the best theoretical work in the privacy area worldwide, they have not often translated into real privacy protections for individuals. For example, the National Information Infrastructure Advisory Council put together a set of principles in 1995 agreed upon by industry, privacy advocates and government officials, yet these principles have not been used since their creation.

In developing a new commission, we urge the committee to:

- carefully examine the work of the past federal commissions — as detailed in Section II, there has been much excellent work that need not be duplicated — and narrow the new Commission's scope accordingly and
- urge that existing privacy legislation in the Internet, medical and financial sectors move forward, resisting suggestions to use this new commission to delay areas that have been under examination for decades.

CDT would like to see **four specific areas** examined in detail:

1) Updating the Privacy Act of 1974

As mentioned in HR 4049, the Privacy Act of 1974 was designed to protect the personal records of individuals held within the federal government and halt the spread of the Social Security Number as an identifier. As early as 1977, a Congressionally-appointed Commission found that the Privacy Act was not as effective as Congress had hoped. [9] To make matters worse, the Office of Management and Budget (OMB) has not updated its Privacy Act Guidance since a year after the Act passed.

The advent of the Internet requires that the Privacy Act be revisited. A 1997 OMB Watch study showed that government Web sites were clearly violating the Privacy Act,[10] and an April, 1999 CDT study showed that only a third of government agencies had privacy policies on their Web sites.[11] With an OMB report on agency compliance with the Privacy Act and a GAO study on privacy notices on Government Web sites expected soon, now seems an ideal time for a Congressional Commission to work with the National Institute of Standard's Computer Systems Security and Privacy Advisory Board to move the Privacy Act into the 21st century.

---

[9] Privacy Protection Study Commission. 1977. Personal Privacy in an Information Society. Washington, DC: Government Printing Office.

[10] OMB Watch. "A Delicate Balance: The Privacy and Access Practices of Federal Government Web Sites." August, 19997. http://ombwatch.org/ombw/info/balance/exec.html

[11] Center for Democracy and Technology. "Policy vs. Practice: A Progress Report on Federal Government Privacy Notice on the World Wide Web." April, 1999. http://www.cdt.org/privacy/fedprivacystatus.shtml

2) Public Records[12]

The issue of public records is a difficult one. Members of this subcommittee, with jurisdiction over both the Privacy Act and the Freedom of Information Act, know that decisions must often be made to balance the important democratic principles of privacy and openness. However, these two great American values need to be looked at not as competitors, but as teammates, in as much as they both lead to greater government accountability. The Internet age has shown that we can no longer assume that just because a record that reveals personally identifiable information is stored in a dusty back room, it is protected. Similarly, government documents currently not exempt in any way, should be on the Internet and open to view — a process that has failed to date.[13] A commission could help Congress, and this subcommittee in particular, examine how to insure that privacy is protected while undertaking the process of making government more accountable by putting more government documents online.

Most public records are at the state and local level. Almost two years ago, Vice President Gore called for a dialogue between states and the federal government to address these issues.[14] While some basic education seems to be under way, no results or information from this dialogue are publicly available. A commission that met in various locations around the country, such as the one proposed in HR 4049, would be in a much better position undertake the task at hand.

3) Access and Security

The principles of access and security are agreed upon fair information practices, but definitions and implementations of these practices vary widely. The Federal Trade Commission (FTC) Advisory Committee on Online Access and Security was created to begin to build consensus on the most difficult of these issues. The Advisory Committee is due to issue its final findings in the form of guidance to the FTC next month. The Commission proposed in HR 4049 could review the work of the Committee and look into how it can most effectively be implemented in both the public and private sectors.

4) Individual Right of Action

Existing federal privacy law has had difficulty allowing Americans redress when a privacy violation has been found. In particular, Privacy Act cases are rarely brought to court because of the barriers for individuals to show both harm as well as a direct

---

[12] Public records that contain personally identifiable information include, but are not limited to: drivers licenses, driving records, motor vehicle registration and titles, property tax records, voting registration records, occupational licenses, use licenses (eg, ham radio, CB radio), firearms permits, court records (eg., bankruptcy, divorce), law enforcement records, political contributions, Security and Exchange Commission filings, financial disclosure filings, hunting and fishing licenses, US Postal Service address records, and vital statistics.

[13] A CDT and OMB Watch joint report entitled "Ten Most Wanted Government Documents" details some of the failures of EFOIA and other federal open records laws
---- http://www.cdt.org/righttoknow/10mostwanted/

[14] http://www.cdt.org/privacy/gore_press.980811.html

violation of the law.[15] It is difficult to say what should happen after a privacy violation since the costs to the individual are not easy to measure and often permanent — once information is out in the world it is hard to bring it back. While the importance of the individual right of action plays an important role in allowing citizens to actively protect their own privacy, we must also examine the ideas of regulatory and non-regulatory privacy agencies, which could be more effective in investigating and highlighting invasive practices in both the public and private sectors. The Commission should examine this issue and provide Congress with recommendations on redress for the future.

While these four areas may not be a complete list of the issues that a Congressional Commission should examine, they represent the type of vital concerns that need to be looked into in greater detail.

Commission Structure

CDT is also concerned that the Commission is currently too time consuming for organizations with limited staff resources. The Commission is set to have 20 hearings in 18 months. The staff time in travel alone from any organization willing to commit to participate would be overwhelming. This is particularly difficult for civil liberties and consumer groups who already have resource difficulties. A modified schedule of 12 or 8 meetings (3 or 2 in each geographical region) in 18 months seems more appropriate.

Conclusion

The Internet privacy legislation currently in front of Congress cover a wide range of issues. Many of these have been well documented in work undertaken by previous commissions and advisory boards. Studying privacy to map protections for the future must remain a high priority and should continue to explore new areas. A commission that would take on the more difficult issues facing privacy would be welcomed. However, such a commission must not be allowed simply to derail legislative hearings and actions on privacy for another 18 months as daily stories of privacy invasions and consumer concerns continue to multiply. While the commission is doing its important work in the areas outlined above, we hope that you will join us in working on ensuring greater corporate and government responsibility, privacy enhancing technologies and legislative efforts to protect privacy.

---

[15] The difficulties that individuals have had are well documented in the "Civil Remedies" section U.S. Department of Justice Office of Information and Privacy's Freedom of Information and Privacy Act Overview. September 1998 Edition. p. 711.

Appendix

A History of Federal Government Privacy Commissions, Workshops and Advisory Boards in the Digital Age

The following is a partial listing of federal government privacy initiatives and the resulting recommendations over the past 30 years. While the focus here are initiatives that directly affect the privacy of government and online services, there have also been a large number of health privacy and several financial privacy initiatives.[16]

1970- 1979

Health Education and Welfare Advisory Committee on Automated Personal Data Systems, 1972[17]

In 1972, Elliot L. Richardson, then Secretary of the U.S. Department of Health Education and Welfare (HEW), appointed an Advisory Committee on Automated Personal Data Systems to explore the impact of computerized record keeping on individuals. In the committee's report, published a year later, the Advisory Committee proposed a Code of Fair Information Practices. These practices have been the basic element for all future Fair Information Practices and future U.S. laws, including the Privacy Act of 1974.

The basic principles of the 1973 Code are as follows:

> 1. There must be no personal data record-keeping systems whose very existence is secret;
>
> 2. There must be a way for an individual to find out what information is in his or her file and how the information is being used;
>
> 3. There must be a way for an individual to correct information in his or her records;
>
> 4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
>
> 5. There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

Privacy Protection Study Commission of 1977[18]

In 1977, at the height of the initial controversy over the legality of computer matching, the Privacy Protection Study Commission, charged with studying the issues raised by the Privacy Act and recommending future legislation, issued its report: Personal Privacy

---

[16] A more complete detailed summary will be available in Priscilla Regan's "Changing Institutional Roles and Responsibilities," a book chapter for Information Privacy: Looking Forward, Looking Back, edited by Mary Culnan, Robert Bies, and Michael Levy (forthcoming: Georgetown University Press).

[17] United States Department of Health, Education and Welfare. 1973. Records, Computers and the Rights of Citizens. Washington, DC: Government Printing Office.

[18] Privacy Protection Study Commission, 1977.

in an Information Age. The Commission was created by the Privacy Act in a provision adopted during final negotiations and accepted as less controversial than creating an Executive branch oversight agency.

The Commission's report recommended that the Privacy Act be more vigorously enforced, and suggested a number of ways to make the Act more effective. The Commission found that the Privacy Act did not lead to the benefits originally expected from the passage of the Privacy Act. The report included a proposed revision of the Act that clarified ambiguities, provided individuals with broader remedies, and tightened the exemptions in the Act. The Commission also recommended that Congress pass additional information privacy legislation to protect information held in private sector databases. Including a set of Fair Information Practices that employers would voluntarily follow when collecting data about individuals for hiring purposes and have served as a basis for many subsequent guidelines.

The Fair Information Practices from the report are as follow:

1. Disclosures of Personal Employment Data

An employer should limit external disclosures of information in records kept on individual employees, former employees, and applicants; it should also limit the internal use of such records.

2. Individual Access

A. An employer should permit individual employees, former employees, and applicants to see, copy, correct, or amend the records maintained about them, except highly restricted security records, where necessary.

B. An employer should assure that the personnel and payroll records it maintains are available internally only to authorized users and on a need-to-know basis.

3. Informing the Individual

A. An employer, prior to collecting the type of information generally collected about an applicant, employees, or other individual in connection with an employment decision, should notify him/her as to:

(1) the types of information expected to be collected;

(2) the techniques that may be used to collect such information;

(3) the types of sources that are expected to be asked;

(4) the types of parties to whom and circumstances under which information about the individual may be disclosed without his authorization, and the types of information that may be disclosed;

(5) the procedures established by statute by which the individual may gain access to any resulting record about himself;

(6) the procedures whereby the individual may correct, amend, or dispute any resulting records about himself.

B. An employer should clearly inform all its applicants upon request, and all employees automatically, of the types of disclosures it may make of information in the

records it maintains on them, including disclosures of directory information, and of its procedures for involving the individual in particular disclosures.

4. Authorizing Personal Data Collection

No employer should ask, require, or otherwise induce an applicant or employee to sign any statement authorizing any individual or institution to disclose information about him, or about any other individual, unless the statement is:

(1) in plain language;

(2) dated;

(3) specific as to the individuals and institutions he is authorizing to disclose information about him;

(4) specific as to the nature of the information he is authorizing to be disclosed;

(5) specific as to the individuals or institutions to whom he is authorizing information to be disclosed;

(6) specific as to the purpose(s) for which the information may be used;

(7) specific as to its expiration date, which should be for a reasonable period of time not to exceed one year.

5. Medical Records

A. An employer that maintains an employment-related medical record about an individual should assure that no diagnostic or treatment information in any such record is made available for use in any employment decision. However, in certain limited circumstances, special medical information might be so used after informing the employee.

B. Upon request, an individual who is the subject of a medical record maintained by an employer, or another responsible person designated by the individual, should be allowed to have access to that medical record, including an opportunity to see and copy it. The employer may charge a reasonable fee for preparing and copying the record.

C. An employer should establish a procedure whereby an individual who is the subject of a medical record maintained by the employer can request correction or amendment of the record.

6. Use of Investigative Firms

Each employer and agent of an employer should exercise reasonable care in the selection and use of investigative organizations, so as to assure that the collection, maintenance, use, and disclosure practices of such organizations fully protect the rights of the subject being investigated.

7. Arrest, Conviction, and Security Records

A. When an arrest record is lawfully sought or used by an employer to make a specific decision about an applicant or employee, the employer should not maintain the records for a period longer than specifically required by law, if any, or unless there is an outstanding indictment.

B. Unless otherwise required by law, an employer should seek or use a conviction record pertaining to an individual applicant or employee only when the record is directly relevant to a specific employment decision affecting the individual.

C. Except as specifically required by federal or state statute or regulation, or by municipal ordinance or regulation, an employer should not seek or use a record of arrest pertaining to an individual applicant or employee.

D. Where conviction information is collected, it should be maintained separately from other individually identifiable employment records so that it will not be available to persons who have no need of it.

E. An employer should maintain security records apart from other records.

8. General Practices

An employer should periodically and systematically examine its employment and personnel record-keeping practices, including a review of:

(1) the number and types of records it maintains on individual employees, former employees, and applicants;

(2) the items of information contained in each type of employment record it maintains;

(3) the uses made of the items of information in each type of record;

(4) the uses made of such records within the employing organization;

(5) the disclosures made of such records to parties outside the employing organization;

(6) the extent to which individual employees, former employees, and applicants are both aware and systematically informed of the uses and disclosures that are made of information in the records kept about them.

While these principles have become a basis for future initiatives, several of the most important recommendations of the Commission — particularly on the Privacy Act of 1974 and laws covering private sector information — have largely been ignored.

1980 - 1989

Organization for Economic Cooperation and Development Guidelines (OECD) on the Protection of Privacy and Transborder Flows of Personal Data[19]

In late 1980, the OECD issued Guidelines concerning privacy. The US provided input through a private sector government collaboration headed by the National Telecommunications Infrastructure Administration (NTIA) in the Department of Commerce and the Bureau for International Communications and Information Policy in the State Department.[20]

Although broad, the OECD guidelines set up important standards for future governmental privacy rules. These guidelines underpin most current international

[19] http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM
[20] Regan, Forthcoming

agreements, national laws, and self-regulatory policies. Although these guidelines were voluntary, about half of OECD member-nations had already passed or proposed privacy-protecting legislation in 1980. The United States endorsed the OECD Guidelines. By 1983, 182 American companies claimed to have adopted the standard although very few ever implemented practices that mapped to the guidelines.

The OECD Guidelines are as follows:

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

The principles remain an international standard for privacy in the computer age.

Computer System Security and Privacy Advisory Board (CSSPAB)[21]

In 1987 Congress established the CSSPAB as a public advisory board as a part of the Computer Security Act. The Computer Security Act specifies that the Board's mission is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

The CSSPAB is composed of twelve members, in addition to the Chairperson, who are recognized experts in the fields of computer and telecommunications systems security and technology. The board examines those issues affecting the security and privacy of sensitive unclassified information in federal computer and telecommunications systems. The CSSPAB's authority does not extend to private-sector systems or federal systems which process classified information.

The CSSPAB advises the Secretary of Commerce and the Director of the National Institute of Standards and Technology (NIST) on computer security and privacy issues pertaining to sensitive unclassified information stored or processed by federal computer systems. The Board reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and appropriate committees of Congress.

1990 - 2000

National Information Infrastructure Advisory Council

In March 1995, the National Information Infrastructure Advisory Council, led by Secretary Ronald Brown at the Department of Commerce, was composed of 37 members, mostly from the private sector, was organized into three 'Mega-Projects' including one on privacy, security, and intellectual property. The Privacy project developed a set of Principles issued in the larger report entitled: "Project Common

[21] http://csrc.nist.gov/csspab/

Ground."

The NIIAC Principles are as follows:

1 For the potential of the NII to be realized, personal privacy - including information, transactions, and communications - must be protected in the design, management, and use of the NII. Autonomy and individual choice are fostered by ensuring privacy and by requiring informed consent prior to the use of personally identifiable information on the NII.

2 Protection of privacy is crucial to encouraging free speech and free association on the NII; however, such protections are not absolute and must continue to be balanced, where appropriate, by concepts of legal accountability and First Amendment rights.

3 To achieve its full potential, the NII must incorporate technical, legal, and self-regulatory means to protect personal privacy. The privacy of communications, information, and transactions must be protected to engender public confidence in the use of the NII. For instance, people should be able to encrypt all lawful communications, information, and transactions on the NII. Network-wide and system-specific security systems that ensure confidentiality, integrity, and privacy should be incorporated into the design of the NII. In an interactive electronic environment, transactional information should be afforded a high level of protection.

4 Existing constitutional and statutory limitations on access to information, communications, and transactions such as requirements for warrants and subpoenas, should not be diminished or weakened and should keep pace with technological developments. Privacy protections should be consistent across technologies, and should be technology neutral.

5 At a minimum, existing rights to review personally identifiable information and the means to challenge and correct inaccurate information should be extended into the NII.

6 Individuals should be informed, in advance, of other uses and disclosures of personally identifiable information provided by that individual or generated by transactions, to which that person is a party, on the NII. Personally identifiable information about an individual provided or generated for one purpose should not be used for an unrelated purpose or disclosed to another party without the informed consent of the individual except as provided under existing law.

7 Data integrity - including accuracy, relevance, and timeliness of personally identifiable information - must be paramount on the NII. Users of the NII, including providers of services or products on the NII, should establish ways of ensuring data integrity, such as audit trails and means of providing authentication.

8 The use of a personal identification system administered by any government should not be developed as a condition for participation in the NII.

9 Subject to public policies intended to secure and maintain the integrity and enforceability of rights and protections under U.S. laws - such as those concerning intellectual property, defamation, child pornography, harassment, and mail fraud - spheres for anonymous communication should be permitted on the NII. Those who operate, facilitate, or are otherwise responsible for such spheres must adequately address the sometimes conflicting demands and values of anonymity, on the one hand, and accountability, on the other.

10 Collectors and users of personally identifiable information on the NII should provide timely and effective notice of their privacy and related security practices.

11 Public education about the NII and its potential effect on individual privacy is critical to the success of the NII and should be provided.

12 Aggrieved individuals should have available to them effective remedies to ensure that privacy and related security rights and laws are enforced on the NII, and those who use the remedies should not be subject to retaliatory actions.

13 The content and enforcement of privacy policy on the NII should be consistent. A process for overseeing the development, implementation, and enforcement of privacy policy on the NII should be established. Such process should receive input from all levels of government and the private sector.

Information Infrastructure Task Force Principles for Providing and Using Personal Information[22]

The technology boom of the 1980s and 1990s caused many countries to review privacy guidelines. New privacy safeguards were needed to correspond with the booming use of computers in data collection. In the U.S., The Information Infrastructure Task Force's (IITF's) Information Policy Committee issued a series of Principles for Providing and Using Personal Information in June 1995. The statement of principles included a call for all participants of the National Information Infrastructure to observe several rules:

- Data should not be altered or destroyed improperly;
- Data should only be collected for a specific purpose and should be kept only as long as it is useful for that
- purpose;
- Inidividuals should be notified about data collection, including why the information is vbeing collected, how it
- will be used, how it will be protected, and what will happen if the data is not provided; and
- Individuals should be able to access and correct their information.

These guidelines where widely criticized by the privacy community as a retreat from the HEW and OECD guidelines.[23]

FTC and NTIA Initiatives

The FTC and NTIA have been more actively involved in addressing online privacy issues since the beginning of the massive growth of the World Wide Web. In April 1995, the FTC staff held its first public workshop on privacy on the Internet, and in November of that year the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues.

In 1995, completed a paper entitled "Privacy and the NII: Safeguarding Telecommunications-Related Personal Information"[24] focused on privacy and online

---

[22] http://www.iitf.nist.gov/documents/committee/infopol/niiprivprin_final.html
[23] See CDT's March 1995 comments to the IITF for an example: http://www.cdt.org/privacy/comments_iitf.html

services. The overall purpose of the paper was to provide an analysis of the state of privacy in the United States as it relates to existing and future communications services and to recommend a framework for safeguarding telecommunications-related personal information. The analysis found "a lack of uniformity among existing privacy laws and regulations for telephony and video services" and recommended "a uniform privacy standard to provide notice and consent" as suggested in the IITF document.

In June 1996, the FTC conducted a two-day workshop to explore privacy concerns raised by the online collection of personal information, and the special concerns raised by the collection of personal information from children. The workshop looked into a wide range of issues including industry self-regulation, technology-based solutions, consumer and business education, and government regulation. The FTC in a December 1996 staff report entitled Consumer Privacy on the Global Information Infrastructure released a report based on the workshops.[25] A second workshop in June 1997 delved more deeply into these issues. As the Commission explained in its 1998 Report to Congress, "in all of these endeavors the Commission's goals have been (1) to identify potential consumer protection issues related to online marketing and commercial transactions; (2) to provide a public forum for the exchange of ideas and presentation of research and technology; and (3) to encourage effective self-regulation."[26]

On June 23-24, 1998, the NTIA held a public meeting on Internet privacy. [27] This meeting was meant to be a dialogue, roundtable and working session with academia, industry representatives, privacy advocates, public interest groups and Washington Policymakers.

The forum addressed the following issues:

- Concerns about privacy in online transactions, Internet browsing and email
- Privacy issues specific to children in the online environment
- The elements of effective self regulation
- A proposed methodology for assessing compliance
- Successful strategies for protecting privacy on the Internet
- Industry developed measures to ensure consumer privacy on the Internet
- Technologies currently available on the Internet to protect consumer privacy

On November 8, 1999, The National Telecommunications and Information Administration ("NTIA") of the United States Department of Commerce and the Federal Trade Commission held a public workshop on November 8, 1999 on "online profiling," the practice of aggregating information about consumers' preferences and interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to create targeted advertising on Web sites. The agencies sought public comment addressing various issues related to the practice of online profiling, thousands of individuals participated.[28]

On March 31, 2000, the FTC hosted the first meeting of the Advisory Committee on Online Access and Security. [29] The purpose of the Advisory Committee is to provide

---

[24] http://www.ntia.doc.gov/ntiahome/privwhitepaper.html
[25] http://www.ftc.gov/reports/privacy/privacy1.htm
[26] http://www.ftc.gov/reports/privacy3/index.htm
[27] http://www.ntia.doc.gov/ntiahome/privacy/confinfo/agenda.htm
[28] http://www.ntia.doc.gov/ntiahome/privacy/index.html
[29] http://www.ftc.gov/acoas/index.htm

advice and recommendations to the FTC on implementation of access and security fair information practices by domestic commercial Web sites. In particular, the Advisory Committee will address providing online consumers reasonable access to personal information collected from and about them and maintaining adequate security for that information. The Committee is expected to finalize its work in May 2000.

Mr. HORN. Thank you very much. We will get back to questions.

Our last panelist on panel two is Sandra Parker, esquire, Director of Government Affairs and Health Policy, the Maine Hospital Association. Thank you for coming down.

Ms. PARKER. Thank you for having me, Chairman Horn. We represent 38 main hospitals and their affiliated entities. I am here today to tell you about Maine's experiences in legislatively protecting the confidentiality of health care information, a small subset of the information referenced in H.R. 4049, but one that is particularly near and dear to us.

Our members, and I think everyone in this room firmly believes that health care information is very private and it needs to be protected against inappropriate disclosures. Dr. Appelbaum did a fine job explaining the reasons and concerns people have, and I am not going to reiterate any of them, but I will tell you in recognition of those concerns, our hospitals have always had policies in place to protect the information, because we think it is important, and we will continue to have the policies, no matter what happens in Augusta, ME or Washington, DC.

The Maine Legislature agreed with us. In fact, they wanted to see every health care practitioner have those practice and policies in places to protect the information, and they felt that the Maine citizens would benefit from a statewide consistent privacy standard in applying to everyone. So they began.

In January 1997, they took up the very difficult task of translating those protective ideals into legislative language. Their initiative would apply only to health care providers in an effort to protect health care information at its source. Respecting the complexity of the task before them, they worked with a professional facilitator and met every 2 weeks with interested parties and a facilitator to exhaustively study the issue and try to anticipate all of the concerns. They worked through the spring, they worked through the summer, they worked through the fall and into the next year. Our dedicated legislators worked for 2 years to develop a bill just on health care information and studied it extensively.

Still, consensus was hard to find, and it wasn't until the final hours of the session in the 1998 session that a compromise bill was quickly passed through the House and Senate. It was to be effective January 1, 1999.

As we reviewed the bill and prepared to help our members comply with the anticipated new law, we began to uncover some unintended and troublesome consequences, despite their extreme hard work.

I would like to just briefly illustrate a couple of those, nowhere near what is in my written statement, but just a quick illustration. To do that, I need to tell you three provisions of the law. First, health care information is defined very broadly and intentionally so. They didn't want any health care information to fall through the cracks. So they defined it as any information that identifies an individual directly and relates to their physical, mental, behavioral condition, medical treatment, personal or family history. It sounds like a terrific definition. We still stand by it, but it caused us some problems.

The second piece I would like you to know is that with certain exceptions, the law required written authorization from the patient or their legally appointed representative before any disclosures could be made. Again, that sounds terrific, and again, it gave us some problems I would like to tell you about.

The third piece you need to know is that written authorization is a defined term in our statute. They specifically denote the elements of a valid authorization and nothing else will do. It must be written and it must have those elements.

Well, nowhere in the law did they reference directory information, and what I mean by that is if you find out that your good friend Sandra Parker is in the hospital and you call the medical center and ask how I am doing they tell you that I am in room 222 and in satisfactory condition. Our law never mentioned directory information, but confirmation that I am in the hospital and saying that I am in satisfactory condition relates to my medical treatment and physical well-being and, therefore, falls within the definition of health care information, therefore requires written authorization from me specifically in order to release it. So, that is what we did. There were delays, however, and when people were in the emergency room and they hadn't gotten to their routine paperwork yet and they said to their care giver could you go out and get so and so from the waiting room, we would have to say, well, no, we can't, because we can't tell them you are here until we get to the paperwork and sign the forms. They could not tell us. Oral authorization was not enough, it had to be written. Unless and until that paperwork was done, visitors couldn't be directed, clergy couldn't be called, phone calls couldn't be transferred, flowers couldn't even be accepted.

It sounds like a good idea, but in practice we received many, many complaints about it.

The idea that oral authorizations were not allowed was a problem for us. Maine residents often spend the harsh winter months in more temperate climes and would like to call their physicians or hospitals and get their medical records transferred and that option was completely removed from their control. They now had to get a special form with statutorily required elements, fill it out, sign it, date it, send it back to their provider before the provider could direct the records to the right place.

The other major problem that we had was that the authorization of disclosure was given only to the patient and their legally appointed representative. That was also done intentionally, for good reason. We don't want anyone else to have control of that information. However, many, many people don't have legally appointed representatives, and by that I mean a guardian, a court-appointed guardian, someone with power of attorney, someone under an advanced directive statute. What we found was that when people didn't have a representative, a legally appointed representative and were unable to sign their paperwork, because they were too ill, they were medicated, they had a stroke, whatever it was, we had nowhere to go. We could release no information to anybody under any circumstances.

So despite great effort, there were some problems. We approached the sponsor of the bill and we worked with her to amend

it, and we submitted a bill, but before the legislature could reach our bill, the law went into effect on January 1, as scheduled, and the day it went into effect, the legislators' constituents began to call, and they called, and called and called and complained, so much so, so adamantly so, that the legislature suspended the law after it was in effect for just 2 weeks and went back to the drawing board. There was extensive discussions about maybe not going forward at all, maybe we should wait for a Federal law, maybe we didn't need it, maybe it was an impossible task. But it was so important, so, so very important that the legislators, to their credit, gave it another try. They worked on it for 6 more months and amended the law.

The amended law went into effect February 1, just a couple of months ago. So far, it seems to be effectively protecting information without provoking consumer outrage. Perhaps we will have more to do. We are still learning our lessons. But it is something that everyone in Maine believes in, and we will keep trying. It is that important.

Thanks.

[The prepared statement of Ms. Parker follows:]

Maine Hospital Association Testimony to the Committee on Government Reform's Subcommittee on Government Management, Information and Technology
April 12, 2000

Good morning, Chairman Horn, Ranking Member Turner, and members of the Subcommittee, I am Sandra Parker, counsel for the Maine Hospital Association, representing 38 Maine hospitals and their affiliated entities. I am here today to discuss Maine's experiences with legislatively protecting the confidentiality of health care information.

Our members, and probably every person in this room, firmly believe that health care information is private information that must be protected against inappropriate utilization or disclosures. We believe that medical confidentiality lies at the heart of caregivers' relationships with their patients. Patients must be assured that the information they share with health care providers will be kept confidential, or they may withhold critically important information. Conversely, health care providers must be able to freely and completely document a patient's health care record, without fear that the information may be used in ways contrary to the patient's best interest. These privacy concerns grow as our health care records contain more and more comprehensive information, such as genetic testing results, and when electronic transmission allows instantaneous, and potentially untraceable, disclosures. In recognition of these concerns, each of our member facilities has always had policies and procedures in place that strive to protect health care information. And they always will....no matter what happens in Augusta, Maine or Washington, D.C.

In January 1997, Maine legislators began the extremely difficult task of translating those ideals into legislative language. This legislative initiative would apply only to health care providers and, therefore, protect the privacy of health care information at its source. Respecting the complexity of the task before them, legislators met with a professional facilitator and interested parties every two weeks for nearly two years, and, confident that their work was complete, hastily passed a compromise bill in the final hours of the 1998 session, to be effective January 1, 1999.

As we helped to prepare our members to comply with the anticipated new law, we began to uncover multiple troublesome and unintended consequences. For example, the statute defined "health care information" very broadly to include any information that directly identifies the individual and relates to the individual's physical, mental, or behavioral condition, personal or family medical history or medical treatment. With certain exceptions, the law also prohibited disclosure of any such health care information without written authorization from the individual, or their legally appointed representative. The statute also specified eight elements of a valid authorization, and prohibited general release forms. The mere combination of these three provisions resulted in the following issues:

- Without specific written authorization from the patient, a hospital could not release "directory" information about an in-patient. Unless and until the patient was able to complete routine paperwork, visitors and clergy could not visit, phone calls could not be connected, and even flower deliveries could not be accepted.
- If a patient could not complete routine paperwork, and had no legally appointed representative, no one could legally authorize any disclosures for any purpose. This untenable situation could occur if an individual was critically ill or injured or became temporarily or permanently incapacitated.
- Without specific parental written authorization, health care providers could not tell school nurses, day care providers, and camp counselors about childhood allergies or immunization histories.
- Without specific written authorization, military officers and relief organizations could not learn about the medical condition of their enlistees or obtain any information to share with an enlistee oversees about the condition of a loved one hospitalized in this country.
- Without specific written authorization, correctional facilities could not learn about the condition of an inmate or gain any information to share with an inmate about the condition of a loved one outside the correctional facility.
- Without specific written authorization, routine medical appointments could not be confirmed by telephone, and test results could not be released over the phone.

- Without specific written authorization, the media no longer had access to the traditional limited "directory" information that was disclosed in the public interest, such as summary conditions of victims of accidents or disasters.
- Without specific written authorization, friends and family members could not purchase or refill a prescription on behalf of a home bound loved one.
- Maine residents traveling out of state could not call for their medical records. They would have to complete and sign a specific written authorization that complied with Maine law, and return it to their health care provider in Maine before their records would be sent as they directed.

Anticipating such problems, the Maine Hospital Association proposed amendments, and our bill was sponsored by Representative Elaine Fuller (D-Manchester) and submitted just prior to the effective date of the new law. However, long before Maine legislators could take up our bill, their constituents began calling to bitterly complain about provisions of the new law. Beginning on the first day the new law took effect, the complaints were so numerous, so adamant, and so unrelenting that the Maine legislature acted with uncommon haste to suspend the law until it could be appropriately amended. This is how we learned that, while we all agreed with the principle of legislatively protecting the privacy of health care information, "the devil is in the details." We found that the ripple effects of implementing this comprehensive law could contradict legislative intent. We discovered that this law affected people we had not anticipated. We learned that we could not accurately anticipate every possible legitimate and necessary disclosure of health care information. We also heard legislators' constituents clearly tell them that the very people they were trying to protect wanted no part of many of the statutory protections. The Herculean task before our state legislature last year, therefore, was to refine the legislative boundaries of "appropriate" disclosures and uses of health care information.

Armed with lessons learned, our legislators worked for another six months to correct these flaws in the original state law. By the end of the legislative session last June, the Maine legislature had extensively debated whether or not to proceed with such a law at all, and if so, how to provide

privacy protection while allowing the necessary and desirable communications with health care providers. In the end, the legislators incorporated their experience into the attached amended law that took effect February 1, 2000. To date, and to the best of my knowledge, the amended law appears to be effectively protecting individually identifiable health information without provoking consumers' outrage.

However, we're *still* learning our lessons. For example, just a few weeks ago, the census workers began arriving at our health care facilities. There is no provision in our law that allows us to release any information to a federal census worker, or to allow them direct access to our patient or resident areas. It is a challenge, but we're doing our best to cooperate with the census takers to the extent we're able to do so, while protecting our patients' health care information and complying with our new state law.

Given our state's experiences, our best advice to anyone considering legislatively protecting the confidentiality of health care information is to move slowly, beware of unintended consequences such as those I have outlined today, and thereby learn from our experiences. Thank you.

Mr. HORN. Well, that is very helpful experience.

Let me ask you, what is the most important privacy issue you have confronted, either with the clientele you represent, or just your own experience? So let's just go down the line, Professor Cate.

Mr. CATE. I guess I would say the single most important privacy issue is trying to find a solution to problems that are not clearly defined. So we talk about opt in and opt out, and things like this. In other words, we have a lot of terms on one side of the equation, tools for protecting privacy, without being clear about what it is we are trying to accomplish. I think that was exactly the issue Congress faced with Gramm-Leach-Bliley.

Mr. HORN. Mr. Plunkett.

Mr. PLUNKETT. Well, I will stick with our theme since it is our focus on financial privacy. One of the things I didn't mention which has been touched on by a lot of the speakers and is in our testimony is that the standards, the principles, the building blocks, if you will, for strong privacy protection are fairly well-known. In fact, they are reflected in the 1974 Privacy Act. They are called fair information practices. One of the most important is that the information that you provide should not be used for a secondary purpose. That obviously means for a purpose other than for which it was given.

Our concern, once again, with financial institutions is that if you open a bank account, you may not know that your bank is affiliated or soon will be affiliated with an insurance company, and there are abuses that can occur there, and I think the NationsBank/NationsSecurities example I gave illustrates that. But there are also problems when cross marketing occurs, because that insurance company, in our opinion, shouldn't have your account transaction and experience information, because that is not the purpose for which you gave them the information.

So to answer your question, I think applying the fair information practices to all of these issues, it can get complicated when you are dealing with the details, no doubt. But the hardest thing for us is to ask people to back up and say, well, don't forget the principles. They are fairly well established, they are fairly well-known, accepted, and please use them.

Mr. HORN. Mr. Schwartz.

Mr. SCHWARTZ. I would say I have three areas. First, children's privacy is very important, because they—it has been shown that they are not really sure what they are consenting to when they actually do consent to something, medical privacy, because the information is so vital, and last information that is held by the government, because there are so many vital services that are needed when you turn over that type of information.

So those three areas are really in terms of if you are going to do a tiered approach, those three areas would be the first place to focus in our minds.

Mr. HORN. Ms. Parker.

Ms. PARKER. At least from our experience, the most difficult piece of protecting this information was the balance, the balance between necessary and desirable communication and the balance against the time that it took to get written authorizations to release the information.

Mr. HORN. Well, I thank you for those answers. I noticed in one of the papers here, I believe it was Mr. Schwartz' one, where you noted the updating of the Privacy Act of 1974, and you made a point here that the quote, to make matters worse, the Office of Management and Budget has not updated its Privacy Act guidance since a year after the act was passed.

What do you feel is the reason for that, and what do you think they ought to do in updating?

Mr. SCHWARTZ. Well, it has only been a year since the OMB has gotten a Chief Counsel for Privacy, so hopefully we are moving down that path. This past year we also had all of the agencies right there on Privacy Act implementation, where they stand on the reports, and the OMB and the Chief Counsel for Privacy in particular will be handing out a final report based on those to the Congress.

Also, GAO is looking into privacy-owned government Web sites, another important issue that should be covered by the Privacy Act more than it is, but as I said in my written statement, the Internet—the Privacy Act wasn't designed with the Internet in mind. So we really do need to reexamine the Privacy Act. I think this kind of commission would be a perfect venue to do that, and it certainly would be great to have more oversight hearings on the Privacy Act when OMB's report moves forward.

Mr. HORN. Mr. Plunkett, is there legitimate need to exchange information between the banks and third-party affiliates, specifically for the various life needs, like check printing and credit billing in small community banks, and wouldn't you agree that these need to be known before laws are enacted which could have unintended consequences, which could cripple entities such as the small community banks?

That is a question that Mr. Hutchinson has left for me to ask, because he had to go to another meeting.

Mr. PLUNKETT. That is a good question. The legislation that Mr. Markey and Mr. Barton have introduced allows for explicit approval for the financial institutions to share information when it is for the intended purpose; that is, if you are opening up a checking account, they can certainly share your checking account information to those that are printing your checks. That is a fairly, I think a fairly easy problem to fix and absolutely there is a legitimate reason in that circumstance to share information.

Mr. HORN. Any other comments on that by anybody? Professor Cate.

Mr. CATE. If I may just say, Mr. Chairman, I think the difficulty here is that there are a lot of uses that we might consider valuable that aren't that immediately obvious. For example, fraud prevention or detection, monitoring accounts to determine if there are charges out of the ordinary, monitoring an account to determine whether that customer is speaking to a balance in a noninterest-bearing account—these are all things which we could debate on whether it is within the purpose for which the person originally disclosed the information. I think we would also all consider them to be valuable uses. I think this really sort of highlights the complexity here.

I obviously disagree that this issue has been thoroughly and well studied and we now know what to do and should do it. I think the

fact that you have 22 States that have introduced 22 different bills, none of them agree on what to do and how to do it, and in fact a large part of that is that we have so little sense, I think exactly what the Maine experience showed. It was easy to focus on the privacy side; it was very hard to focus on what are all the valuable, useful things we do with useful information every day that we don't want to put a stop to.

Mr. HORN. Thank you. Well, thank you. I just have one question before I yield to Mrs. Maloney.

Some of you have had experience on the privacy laws abroad, and I am curious what your thinking is on the European Community's privacy laws. You will recall the European Community asked all of their Member States to put together a privacy law about 2 years ago, and then they put it off for a while, and there were real concerns in this country in terms of the free flow of data between corporations of the United States subsidiaries in Europe and European subsidiaries in the United States, and that was one of the reasons they put it off.

I just wondered what your thinking is there, and would that have made a major impact on the economy. Again, they wanted, I guess even a census date that the individual signed the form, which sounded a little much. But go ahead.

Mr. CATE. Well, Mr. Chairman, thank you. I think the answer is absolutely it would have made an enormous impact on not only the economy of international trade between the United States and Europe, but also within Europe, which is probably why Europe has really not implemented the directive. Half of the countries haven't implemented it at all, they have not even made the pretense of implementing it. The others have implemented laws which we are told by data protection commissioners in Europe are not being enforced currently.

So, for example, if you read the law, what is the law today in England, Greece, or Portugal, it would tell you that the law is opt in affirmative consent. You must get consent, for example, from every employee in writing before you process their data. What we know is that is not taking place in any of those countries, that in fact they are simply using a slightly different mechanism than we use. We tend to write exceptions into law; they are simply putting those exceptions into practice.

Mr. HORN. Any comments on that, Mr. Plunkett?

Mr. PLUNKETT. I would note that in the so-called safe harbor negotiations, many of the same entities, financial institutions in particular, that talk about the expense of complying with meaningful privacy protections, and by that I mean privacy protections that extend to affiliates which I spoke about earlier and information-sharing to affiliates, many of the same companies that are objecting there are willing to go along with an agreement that is close to being consummated, the so-called safe harbor agreement, that will provide European customers of American institutions with greater privacy protection than with American customers.

Mr. HORN. Now I yield to the gentlewoman from New York. It is good to see her here, a former ranking member.

Mrs. MALONEY. Great to see you, Mr. Horn, and thank you for calling this important hearing. I would like to request that my opening statement be put in the record.

Mr. HORN. Without objection, it will be put where all the opening statements were, as if read.

Mrs. MALONEY. Thank you. Then I would like to just ask a few questions. I am not against this bill, but I hope that the intent is not to stop other protections from going forward, and the protections that we already have in place.

Last year, as a member of the Banking Committee, I had an opportunity to participate in the conference on the Gramm-Leach-Bliley Financial Services Reform Act where we had a considerable debate over issues related to the privacy of financial institutions and passed some privacy protections for consumers of financial institutions. These regulations have not even been in place yet. Shortly over 2 billion consumers will be receiving privacy notices in the mail, and my question is, would this commission in any way halt or hinder this work that we have already done? This commission?

Mr. CATE. Well, if I can speak to that, I would say certainly, you know, our view is that it should not.

Mrs. MALONEY. So it would not. Is that clear in the bill?

Mr. CATE. I believe there is no language in the bill that would suggest it has the power to stop the implementation or that it is the intent of Congress to stop the implementation of any existing law. You might even argue further, I mean this would suggest to me why, if the commission goes forward, you would probably want people on it, some of the members of it, to be involved in the implementation of that law, to bring the experience of that process to the commission.

Mrs. MALONEY. I would like to mention——

Mr. PLUNKETT. Could I respond as well?

Mrs. MALONEY. Sure. Anybody can comment.

Mr. PLUNKETT. I would agree that the intent of the act is not to inhibit implementation of the Gramm-Leach-Bliley act. I would note, though, that the regulations that are ongoing don't deal with the significant flaw in the act that these State bills and the Federal bills have identified, which is the affiliate-sharing loophole.

Mrs. MALONEY. But a number of States are going forward with their initiatives, as I understand it, is that correct?

Mr. PLUNKETT. Well, they are moving through the process, including in New York, from what I understand.

Mrs. MALONEY. Now, I would like to ask about another issue. We actually had several hearings on this particular matter, the Health Insurance Portability Act, a 1996 act. It provided that if Congress was not able to reach consensus and enact legislation on medical privacy by August 1999, the Secretary of Health and Human Services would come forward with medical privacy regulations to ensure that Federal medical privacy protections are in place. Since Congress failed to meet the August 1999 deadline, the Secretary is now, as we sit here, in the process of finalizing medical confidentiality regulations.

I would just like to ask the members of the panel, do you believe that if a privacy commission were created, the administration should delay moving forward with these regulations until after the

commission completed its report? I would like to really—you know, in other words, the question I am asking is one that—would this in any way hinder work that is already in place from going forward or stop other protections from going forward?

I don't know if the proper person to ask is the panel or Mr. Hutchinson himself, but you know, the fact that we have been working in this committee actually since 1996 and that these are supposed to come forward, I believe, shortly, would this in any way hinder that from going forward in?

Mr. HUTCHINSON. If the gentlewoman would yield.

Mrs. MALONEY. Absolutely.

Mr. HUTCHINSON. The answer is no. There was some discussion and some urging to put in the commission bill a moratorium on other regulations and legislation moving forward until the commission did its work, and we specifically rejected that, because again, I view this commission and this legislation as complementary and not as a substitute. So there would not be a prohibition there. In fact, I think many of those will be adopted this year, won't they?

Mrs. MALONEY. Well, yes, they are supposed to come forward, and as we mentioned while you were not in the room, the financial services bill, the bipartisan Leach-Bliley bill had privacy for the financial institutions, and they are in the process of coming forward with them, and as I mentioned, roughly 2 billion consumers will be getting notices. This will not in any way hinder the work of the Banking Committee on the privacy issue?

Mr. HUTCHINSON. The answer is it will absolutely not interfere.

Mrs. MALONEY. Now, obviously, who is on this commission is going to have a lot to do with how well it operates. I understand from reading it that there is no criteria for the commission's membership.

I would just like to ask Mr. Cate, Mr. Plunkett, and Mr. Schwartz, what are your ideas of criteria for membership on this, and what do you think would be the appropriate criteria for membership on the commission?

Mr. SCHWARTZ. I will address that, partly because I addressed it in my written testimony and was not able to address it orally.

Mrs. MALONEY. I am sorry. I missed it then.

Mr. SCHWARTZ. We think that it is very important that consumer groups, privacy advocates, and the other—along with many of the other groups that would be affected in the financial health industries be represented on the panel. We have specific concerns that the schedule for the panel, 20 meetings in 18 months, is really quite a heavy load for—particularly for consumers groups and civil liberties groups, because even the time constraints on limited staff resources can be very difficult, so we hope that that can be addressed as well.

Mr. CATE. If I may also respond and wholly join in that comment, I think one of the assumptions is that if a commission goes forward, it has a tremendous amount of deliberation to do, that it is not so much unearthing new information, it is working out ways of working with existing information. I think one of the things that would be of concern in the bill is the requirement for 20 hearings in five different locations in 18 months, that it would be preferable to have this commission be able to spend a greater amount of its

time in deliberation as to how to reconcile these issues as opposed to engage quite so much as a fact-finding body.

If I may also just add one point: in addition to the representation along types of groups, consumer groups, industry groups and so forth, I too would reiterate the point that I think it is important that the experiences that the members bring to the table, whether those are experiences from business or industry or consumer groups or academia, it makes no difference, that those experiences reflect a broad range of interests and approaches to privacy; that what you don't want is a group of people who are all focused on privacy, but just from different points of view, since we have clearly I think come to understand that these privacy issues touch on, as the Maine experience shows, so many other realms of our lives that you would want that well represented.

Mrs. MALONEY. Just as a followup, Mr. Cate, in reading your testimony, you stated that the commission's work might duplicate the Treasury study on Gramm-Leach-Bliley on financial privacy. Do you think that the commission is unnecessary as a whole, or just unnecessary with regards to the financial services industry? Could you sort of clarify your thoughts on that?

Mr. CATE. Yes. Unfortunately, I can only make them as clear as they are, and you may find that they are somewhat befuddled to start with. I think it is very important that the commission not duplicate existing work, and I think there is a real risk with the Treasury study under way currently that you would not want the commission to do the same type of study.

Mrs. MALONEY. When is the Treasury supposed to complete their study, do you know exactly?

Mr. CATE. I believe they have another full year to complete it. So there would be some overlap potentially between the commission and the Treasury study. That is true in other areas as well. I mean there are certainly other studies and other studies done in the past. I don't think you want any of those duplicated.

I think that doesn't put an end to the question, though. The question is, if there is a commission, how can it build on the work that the Treasury is doing. There would be a variety of ways. I mean one way would be to exclude financial information, to say look, the Treasury has been dealing with that, we are going to leave that out. Another way would be to say include financial services information, but with particular attention to not sort of going through the same types of hearings, the same types of deliberation, but rather to draw on what the Treasury and other financial regulators are doing. I am sure there are many other ways of doing that. That is instruction it seems to me Congress would want to give either through legislative history or the legislation.

Mrs. MALONEY. Is my time up, Mr. Chairman?

Mr. HORN. Go ahead.

Mrs. MALONEY. Thank you, Mr. Chairman.

You made a statement about the valuable—useful use of information, and I think one of the most startling things in our country now, and really in our economy and in our life, is just the fast-changing pace of the so-called information age. We have had hearings on many of the things that may be driving these tremendous, or one component, the tremendous success of our economy is this

whole information age that is allowing so much to happen so quickly.

Would you elaborate in your statement on really not wanting to curtail the use of information and being able to grow on this new phenomena, but also to protect privacy and some of the valuable, useful uses of information that we don't want to hinder in the growth of possibilities for individuals and really growth of our country?

Mr. CATE. Well, yes. Thank you. Let me offer two responses. One is I think it is critically important that we do a better job, and by we I mean all of us. Certainly academia bears a shared responsibility, for not having engaged in the type of research as to how we use information. We really know very little about that. We know a lot about privacy, we know very little about, if you will, the infrastructure uses of information. How does a business, how does Congress use information about individuals and in what ways does it benefit our lives? What are ways in which—public records is a good example that was raised earlier. In the financial services context, I think that type of an investigation has really first begun.

I did a study which was published just a month ago now which was just the tip of the iceberg in looking at the types of beneficial uses that come out of allowing relatively unhindered access to basic personal information. Who has an account, where, what do they use it for, etc. The best example of that is probably fraud prevention, that if we can look across accounts, you see patterns of consumer behavior, which then when you see anomalies, may alert the bank or the credit card issuer or whomever to the fact that there is something here that that consumer may need to be notified about or there may need to be further inquiry.

As we heard on the first panel, given that it is the businesses and then ultimately consumers that sustain those losses, that cover those losses where there is fraud, for example, allowing that type of use seems important. But I think the second response was more the process response. I think that is why if there is to be a commission, or if there is not to be a commission, it is important that we all be engaged more in the process of figuring out what are the other uses of this type of information. They may be as pedestrian as confirming where to make a flower delivery for a patient in the hospital, but that really matters to real people who are in distress.

Mr. PLUNKETT. Could I just jump in and say that nothing in any of the financial privacy proposals that we or I believe anybody supports would prevent fraud prevention or inhibit fraud prevention. It is important also to note the increasing, again, uneasiness that Americans have about erosion of their privacy. I do not want anybody to get into this situation where they are putting privacy at odds with economic interests. As I mentioned before, when it comes to, for instance, being at ease with electronic commerce, privacy protection may actually be the best thing for more people using the World Wide Web and the Internet, and taking advantage of electronic commerce because they won't worry that their privacy is being violated.

Mrs. MALONEY. Well, I appreciate your testimony. My time is up. I would just appreciate, Mr. Hutchinson, if in the, I don't know, intent or some place in the bill you would let it be clear that you in

no way want to hinder the work going forward from the 1996 Health Insurance Portability Act on privacy and also the work of the Banking Committee on the Gramm-Leach-Bliley, so that it doesn't hinder this work going forward.

Mr. HORN. We are going to have a markup on this. That might come up there. I will tell you, if this commission doesn't pass, there won't be much passed, because they have had numerous privacy bills in the Senate, in the House; they have gone nowhere, except the one on the banking and the human services regulations issued by the Secretary. So I look on it the other way, that this is the way to get a privacy law on the book, is get that commission moving.

I thank the gentlewoman for being here.

The last word I will give to the prime author of the legislation, Mr. Hutchinson. I want to say that both the Democratic side and the Republican side will be forwarding you and the first panel some questions that we haven't been able to get to. We hope you will write the answers and they will go in this part of the record.

In addition, we will keep the record open to any citizen for the next 2 weeks, roughly 14 days.

So please send it to the staff. It is B–373, I believe. The chief counsel and staff director, Mr. George, is over there, and we will work it out with everybody as to the questions and they will go into the official record.

So I now yield for the last word on this subject for 5 minutes to the gentleman from Arkansas.

Mr. HUTCHINSON. I thank the Chairman. Again, I want to express my appreciation for this hearing, your willingness to schedule a markup on this legislation. I just want to make a couple of comments. First, I want to thank Ms. Parker for being here and testifying on this and giving us the experience from Maine. I think that is very instructive and helpful as we look at this in Congress and our responsibility.

There has been some questions about the criteria for membership, and I would emphasize that, you know, this can be changed; obviously, that is what the markup is for, and if wisdom prevails that we ought to specify different criteria for involvement in this commission, then I am certainly open to that. But the reason that was not included is, as I stated before, there is always a fear of leaving someone out. I can just see itemizing who should belong to this commission and someone coming up and saying, well, how about our group, or how about this particular stakeholder. So you start down a risky path.

The other reason is that it is consistent with other commissions in the past that you leave the particular makeup of the commission to the appointing officials and allowing a bipartisan consensus to develop on it. So I would expect that all of the important stakeholders should be and will be represented on the commission. But again, if we need to be more specific than that, then that might be an option.

The second issue, and I want to talk to Mr. Plunkett for a moment, and I very much appreciate your testimony today, and I specifically wanted you on this panel because I knew you disagreed with the commission. I think it is important as you consider legislation that you hear from both sides. I appreciate your work on pri-

vacy. You and I can get together and we can push some of these bills through and we can get some passed this session, but there are a lot of other players out there, and I think in fact because it could be a short legislative session, it is going to be difficult, as the chairman said, to develop a consensus on an individual bill. But it is very important that this not be used as an excuse not to continue passing some privacy regulations or some privacy initiatives.

I see this as complementary. If you passed everything on your wish list, Mr. Plunkett, this year, I still think we need a privacy commission, because you still have on-line privacy issues, you have developing technology, you have got new criminals out there that create new methods of invading someone's privacy. So I think that we need to see how the laws that we passed are going to work, we need to see how the FTC and the other regulations that are being considered on financial privacy, how they are working out there, and that is part of the function of this commission, to see what supplementary we need to do.

For example, Mr. Plunkett, I mean there is the opt-in, opt-out question right now, am I correct?

Mr. PLUNKETT. Oh, yes.

Mr. HUTCHINSON. And so if there is not—I mean the regulations that are going to be adopted are going to be under the—where you have to specifically opt out, is that correct?

Mr. PLUNKETT. In some cases. In other cases it won't be allowed, yes.

Mr. HUTCHINSON. So if you want to change that, unless we pass some legislation, the commission would have to look at that.

Now, I think the debate was whether we should even look at that at all, because it is already under consideration by an ongoing regulatory body, and I think that is a fair consideration we need to talk about some more. But regardless of what we pass, I see the need for a commission to look at the new challenges in the future, and to look at it comprehensively rather than just sectorially, what are we doing in financial privacy, what are we doing in health care records and what are we doing with on-line. It intersects and cross-sections each other. So that was the purpose of it.

I know that was a little bit of a speech——

Mr. PLUNKETT. After my speech, you have a right.

Mr. HUTCHINSON. So thank you again, Ms. Parker and gentlemen, for your testimony today. I yield back, Mr. Chairman.

Mr. HORN. I thank the gentleman very much. I hear the gentlewoman from New York has one question.

Mrs. MALONEY. Mr. Chairman, I have another item that really came out of the Banking Committee and I would like to ask Mr. Hutchinson for clarification. I would like to see it in this bill, and I am waiting to see the final language, but I am not against this bill and will probably support it.

But one thing that we were very concerned about is that each State is different in their financial services, very different. So States wanted the freedom to come forward with stricter provisions and insurance or privacy or banking or their own special needs, and in your bill, do you see that this would not in any way hinder the ability for States to go forward with stricter provisions?

Mr. HUTCHINSON. No. The commission will have to look at what the States have done, consider their approach, and consider whether you want to have a comprehensive Federal approach, or where you have a Federal floor which is supplemented by the States.

Mrs. MALONEY. That is what we supported in Banking.

Mr. HUTCHINSON. And that would certainly be my inclination, but that is something that the commission would have to debate.

Mrs. MALONEY. Thank you.

Mr. HORN. I thank the gentlewoman. I would like to thank the staff on both sides. Let me just go down the line. The staff director, chief counsel for the House Subcommittee on Government Management is Russell George; the counsel next to me for this particular hearing is Ms. Bailey; Bonnie Heald, director of communications back there; and Bryan Sisk, clerk; and Ryan McKee, staff assistant; Michael Soon, intern; and Mr. Turner's counsel is Trey Henderson, counsel; and Jean Gosa, minority clerk; and Julie Bryan is our faithful court reporter. So thank you very much for being with us.

With that, we are adjourned.

[Whereupon, at 12:20 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

FRED H. CATE

Professor of Law and Harry T. Ice Faculty Fellow
Director, Information Law and Commerce Institute
Senior Counsel for Information Law,
Ice Miller Donadio & Ryan

Indiana University School of Law—Bloomington
211 South Indiana Avenue
Bloomington, Indiana 47405-7001
Telephone (812) 855-1161
Facsimile (812) 855-0555
E-Mail fcate@indiana.edu

April 28, 2000

Via E-mail and Federal Express

The Hon. Stephen Horn
Chairman
Subcommittee on Government Management,
Information, and Technology
Committee on Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Chairman Horn:

Thank you for the opportunity to testify before the Subcommittee on Government Management, Information, and Technology at your April 12, 2000, hearing on H.R. 4049. It was a privilege to appear before you, and I greatly appreciate your leadership on addressing the important issues surrounding the protection of personal privacy in the context of critical information flows that undergird our economy and democracy.

In your letter of April 17, 2000, you asked that I provide additional information in response to two questions:

1. Aside from outright regulation, what steps can be taken to protect privacy by consumer groups, private sector institutions and the Federal Government?

2. What can States do to protect private financial information?

I appreciate the opportunity to address both questions and I will try to do so as briefly and specifically as I can. Unlike my testimony at the hearing, which reflected not only my views but also those of the Financial Services Coordinating Council, these responses should be attributed to me alone.

Nonregulatory Actions

As I am sure you are aware, there are many examples of nonregulatory actions to protect privacy by individuals, businesses, not-for-profit groups, educational

institutions, and government institutions. I will highlight five that I believe are the most important generally, and a sixth category that applies to government activities only.

1. Individual Institution Actions and Policies

For much of this century—long before privacy became a politically sensitive issue—many businesses and other institutions have taken a wide variety of actions designed to protect their customers' privacy and to enhance their customers' ability to protect their own privacy. This is particularly true in the financial services sector, where privacy has long been a key part of the trust that is at the core of successful customer relationships. High levels of physical and computer security for customer data, the use of passwords and personal identification numbers for account access, encryption of computerized data, requiring verification of identity before providing access to account information, restricting internal access to customer data on a need-to-know basis—these are all examples of routinely used, effective measures for protecting personal privacy. These are backed up by strong policies designed to protect sensitive information from inappropriate disclosure.

In response to recent privacy concerns, many institutions have further heightened the protection they extend personal information through enhanced computer security measures, such as firewalls and stronger encryption; new technologies for verifying identity, such as the use of fingerprints; and more restrictive privacy policies, such as requiring callers or Web visitors to provide even more verification of their identity before account information is disclosed to them.

Today, many companies are actively competing for customers by promoting their privacy policies and practices. As we have seen time and time again, when consumers demand better privacy protection, competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much we really value privacy.

2. Self-Regulation

In addition, many industry associations have adopted privacy standards and principles. Corporate compliance with privacy standards constitutes an increasingly important accolade in competitive markets. Moreover, industry associations help persuade member organizations to adopt and adhere to industry norms for privacy protection. The majority of the individual reference services group industry has agreed to abide by the IRSG Principles, which not only establish data protection standards, but also require annual compliance audits by third parties and a commitment not to provide information to entities whose practices are inconsistent with the IRSG Principles. Many

other industry associations, including those in the financial services sector, have adopted similar privacy principles or codes of conduct.

3. Technologies

The very technologies that may enhance privacy concerns, for example the Internet, often provide tools for protecting privacy far more effectively than any law or regulation. For example, technological innovations such as adjustable privacy protection settings in both Netscape and Microsoft Explorer, encryption software, anonymous remailers, and other Internet-based services make it possible to browse anonymously and obtain information via the Web without being identified. These technologies and services make privacy realistically possible for many Americans for the first time ever. Moreover, new technologies and technology-based services to protect privacy are constantly being developed. One new service, soon to be announced publicly, will extend Internet anonymity to allow an individual to make purchases online and ship goods to her home or a drop-off location without ever disclosing her real identity, address, e-mail address, or credit card number to anyone. Unlike the small-town America in which I grew up, where everybody knew everyone else's business, these technologies offer the promise of real anonymity and, as is discussed below, real control over what personal information to disclose and to whom. Similarly, new technologies for using fingerprints and other biometric identifiers, while often criticized as raising privacy concerns, also afford unprecedented new privacy protection by making it possible to verify customer identity, even from remote locations, before disclosing sensitive information.

Technologies can actually and completely protect privacy; law cannot. At best, the law can regulate data collection and use and then impose penalties for users who engage in prohibited practices, but this is only effective if (a) the illegal use is discovered; (b) the use is identified; (c) the user is subject to the law or regulation and within the jurisdiction of an appropriate court or administrative agency; (d) the aggrieved data subject has the wherewithal or obtains the cooperation of a government agency to pursue the data user in court; (e) the aggrieved data subject can prove her allegations in court; (f) a judge or jury agree find the user guilty and assess a fine or other penalty; (g) the penalty can be enforced. As this litany makes clear, while privacy laws and regulations can cause considerable damage to society and the economy, they often provide very little practical privacy protection and none whatsoever against data users outside of the country or bad actors who are unconcerned with the requirements of the law. To the extent we eliminate the incentive for the development of technological protections for privacy, not just online but in other settings, we diminish the availability of real privacy for everyone.

4. Third-Party Privacy Certification Services

The widespread availability, increased power, and decreased price of many technologies also facilitates a vibrant market for privacy protection, such as the online privacy certifications like BBBOn-line and TRUSTe. Similar services operate in the off-line world as well, for example, privacy audits conducted by major accountings firms.

5. Education and Research

Public education is at the heart of any system of privacy protection. Even the most restrictive systems, such as that adopted by the European Union, depends at heart on consumers being well-informed. This is, of course, nothing new. Informed discretion and judgment have long been among the best protections for privacy, but education is assuming new importance today. And that education is the responsibility of all of us—industry, consumer groups, schools and colleges, and the government.

Along with the vital role of education in protecting privacy is the need for more research. Too frequently Congress and state legislatures are being asked to legislate restrictions on information flows without being given access to data on the value of those flows, the impact of those restrictions, and the availability of less costly, more effective alternatives. This is also a responsibility we all share, but the government in particular—through the General Accounting Office, Congressional Budget Office, Congressional Research Service, the Federal Reserve Board, and other agencies—is well placed to help supply the information that you need to determine if further legislation or regulation is necessary to protect privacy and, if so, of what form. In addition, government funding of research concerning privacy and information flows is as necessary as government funding of other forms of medical and scientific research.

6. Nonregulatory Role for the Government

Government action to protect privacy can take many forms other than regulation, including facilitating the measures outlined above, conducting research and education, and providing fora for further discussion of privacy and information flow issues. In addition, there are at least two additional roles that only the government can play.

a. Enforcement Forum

First, the government does and should continue to provide a forum or mechanism for enforcing privacy commitments. That enforcement role includes not only providing accessible courts, but also assisting consumers in enforcing their legal rights and in ensuring compliance with corporate privacy policies. The Federal Trade

Commission fills this role across a broad variety of industries. Exercising the power Congress gave the Commission in the Fair Trade Act to investigate and prosecute "unfair and deceptive practices in or affecting commence,"[1] the Commission has helped to ensure that information users adhere to their privacy policies. (I should also note the significant role that the FTC has played in encouraging companies to promulgate those policies.) In a highly regulated industry like financial services, federal and state financial industry regulators have also played a significant role in encouraging and enforcing privacy policies. So, too, have those state courts that have found implied contracts between financial institutions and their customers concerning the confidentiality of private information.[2]

The success of federal and state government officials in using existing laws to protect privacy is noteworthy and undercuts the argument that new laws are necessary to protect privacy.

b. Preemption

Second, given the importance of information flows and their inherently national—even global—nature, which I discussed in my prior testimony, Congress should restrict the ability of states to enact conflicting privacy laws and regulations. There are two separate reasons for this: (1) Privacy is simply too important and the role of information flows too great to allow each state to adopt its own standards, whatever they may be; and (2) complying with as many as 50 sets of inconsistent privacy laws and regulations confuses consumers and imposes considerable costs on both consumers and businesses without generating any greater privacy protection.

The Gramm-Leach-Bliley Financial Services Modernization Act,[3] by failing to preempt inconsistent state laws, ensures neither a uniform national standard of protection nor a minimum level of access to that information, irrespective of the value served by that access. This may ultimately prove to be its most significant impact on consumers, financial institutions, and the economy—not enhanced privacy protection, but customer confusion as we face inconsistent state laws and regulations and unnecessary costs as businesses comply with those inconsistent requirements.

---

[1] 15 U.S.C. § 57b-1.

[2] See L. Richard Fischer, The Law of Financial Privacy ¶ 5.04[3] (3d ed. 1999) and cases cited therein.

[3] Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, § 507(b).

State Action to Protect Financial Privacy

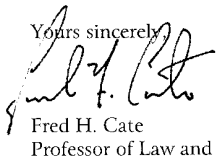
The points outlined above suggest a number of important roles for states in helping to protect the privacy of financial information, as well as some limits to those roles. State courts, for example, are a key forum for citizens to vindicate their privacy rights under existing laws and privacy policies. States also play a critical role in educating the public about privacy issues, especially through consumer protection and public access agencies and through state-funded schools and colleges. States can also help fund the research that is so desperately needed in this area. States can facilitate the development of privacy policies and provide incentives for the development and distribution of privacy-protecting technologies and services. In addition, as you know, states are specifically charged under Gramm-Leach-Bliley with implementing the law as applied to insurance companies.

What I would hope that states will avoid doing—and that Congress will preempt states from doing—is enacting new privacy laws or regulations applicable to national activities, such as the provision of financial services. These laws and regulations are inevitably inconsistent with each other and/or with federal enactments, thereby creating the confusion and imposing the costs identified above.

Obviously, there is more that industry, the not-for-profit sector, and the government can do—short of regulation—to enhance consumer privacy and empower individuals to better protect their own privacy. Further regulation is not only largely unnecessary, it is often almost always both less effective and more expensive in protecting privacy. I appreciate the opportunity to offer these additional comments in response to your questions, and I hope you will not hesitate to call on me again in the future if I can be of assistance.

Thank you again.

Yours sincerely,



Fred H. Cate
Professor of Law and
Harry T. Ice Faculty Fellow

○