AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

H.R. 4049, TO ESTABLISH THE COMMISSION FOR THE COMPREHENSIVE STUDY OF PRIVACY PROTECTION

HEARINGS

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

H.R. 4049

TO ESTABLISH THE COMMISSION FOR THE COMPREHENSIVE STUDY OF PRIVACY PROTECTION

MAY 15 AND 16, 2000

Serial No. 106–204

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

71–178 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*
ROBERT ALLOWAY, *Professional Staff Member*
BRYAN SISK, *Clerk*
MARK STEPHENSON, *Minority Professional Staff Member*

CONTENTS

Page

Hearing held on:
- May 15, 2000 1
- May 16, 2000 93

Text of H.R. 4049 2

Statement of:
- Belair, Bob, editor, Privacy & American Business; Mary Culnan, professor, McDonough School of Business, Georgetown University; Christine Varney, former Commissioner, Federal Trade Commission; Solveig Singleton, Director of Information Studies, CATO Institute; Ron Plesser, legislative counsel, 1977 Privacy Commission; and Stanley Sokul, member, Advisory Commission on Electronic Commerce 115
- Hatch, Mike, Minnesota State Attorney General 33
- Markey, Hon. Edward J., a Representative in Congress from the State of Massachusetts 189
- Spotila, John, Administrator, Office of Regulatory Affairs, Office of Management and Budget 17
- Stone, Robert, executive vice president, American Healthways 41
- Veator, David, Office of Consumer Affairs and Business Regulation, State of Massachusetts 27

Letters, statements, etc., submitted for the record by:
- Belair, Bob, editor, Privacy & American Business, prepared statement of 117
- Culnan, Mary, professor, McDonough School of Business, Georgetown University, prepared statement of 126
- Hatch, Mike, Minnesota State Attorney General, prepared statement of ... 35
- Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of 95
- Moran, Hon. James P., a Representative in Congress from the State of Virginia:
  - Prepared statement of 61
  - Prepared statement of Marjory Blumenthal, Director, Computer Science and Telecommunications Board, the National Academies 55, 109
- Plesser, Ron, legislative counsel, 1977 Privacy Commission, prepared statement of 160
- Singleton, Solveig, Director of Information Studies, CATO Institute, prepared statement of 152
- Sokul, Stanley, member, Advisory Commission on Electronic Commerce, prepared statement of 168
- Spotila, John, Administrator, Office of Regulatory Affairs, Office of Management and Budget, prepared statement of 20
- Stone, Robert, executive vice president, American Healthways, prepared statement of 43
- Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of 108
- Varney, Christine, former Commissioner, Federal Trade Commission, prepared statement of 134
- Veator, David, Office of Consumer Affairs and Business Regulation, State of Massachusetts, prepared statement of 30
- Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of 99

H.R. 4049, TO ESTABLISH THE COMMISSION FOR THE COMPREHENSIVE STUDY OF PRIVACY PROTECTION

MONDAY, MAY 15, 2000

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

The subcommittee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Turner.

Also present: Representatives Hutchinson and Moran.

Staff present: J. Russell George, staff director and chief counsel; Heather Bailey, professional staff member; Bonnie Heald, director of communications; Bryan Sisk, clerk; Liz Seong and Michael Soon, interns; 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, this hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

At the request of the subcommittee's minority members, we will continue our April 12th examination of H.R. 4049, a bill that would establish a Federal commission to study privacy protection.

[The text of H.R. 4049 follows:]

I

106TH CONGRESS
2D SESSION

H. R. 4049

To establish the Commission for the Comprehensive Study of Privacy Protection.

IN THE HOUSE OF REPRESENTATIVES

MARCH 21, 2000

Mr. HUTCHINSON (for himself, Mr. MORAN of Virginia, Ms. GRANGER, Mr. BRADY of Texas, Mr. DAVIS of Florida, Ms. PRYCE of Ohio, Mr. SUNUNU, Mr. BARRETT of Wisconsin, Mr. COBURN, Mr. DICKEY, Mr. KLECZKA, Mr. PITTS, Mr. GREENWOOD, Mr. RILEY, Mr. DUNCAN, Mr. LUCAS of Oklahoma, Mr. KOLBE, Mr. CAMPBELL, Mrs. KELLY, Mr. DAVIS of Virginia, and Mr. VITTER) introduced the following bill; which was referred to the Committee on Government Reform

---

A BILL

To establish the Commission for the Comprehensive Study of Privacy Protection.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Privacy Commission Act".

SEC. 2. FINDINGS.

The Congress finds the following:

1 (1) Americans are increasingly concerned about
2 their civil liberties and the security and use of their
3 personal information, including medical records, edu-
4 cational records, library records, magazine subscrip-
5 tion records, records of purchases of goods and other
6 payments, and driver's license numbers.
7 (2) Commercial entities are increasingly aware
8 that consumers expect them to adopt privacy policies
9 and take all appropriate steps to protect the per-
10 sonal information of consumers.
11 (3) There is a growing concern about the con-
12 fidentiality of medical records, because there are in-
13 adequate Federal guidelines and a patchwork of con-
14 fusing State and local rules regarding privacy pro-
15 tection for individually identifiable patient informa-
16 tion.
17 (4) In light of recent changes in financial serv-
18 ices laws allowing for increased sharing of informa-
19 tion between traditional financial institutions and in-
20 surance entities, a coordinated and comprehensive
21 review is necessary regarding the protections of per-
22 sonal data compiled by the health care, insurance,
23 and financial services industries.
24 (5) The use of Social Security numbers has ex-
25 panded beyond the uses originally intended.

1 (6) Use of the Internet has increased at as-
2 tounding rates, with approximately 5 million current
3 Internet sites and 64 million regular Internet users
4 each month in the United States alone.
5 (7) Financial transactions over the Internet
6 have increased at an astounding rate, with 17 mil-
7 lion American households spending $20 billion shop-
8 ping on the Internet last year.
9 (8) Use of the Internet as a medium for com-
10 mercial activities will continue to grow, and it is esti-
11 mated that by the end of 2000, 56 percent of the
12 companies in the United States will sell their prod-
13 ucts on the Internet.
14 (9) There have been reports of surreptitious
15 collection of consumer data by Internet marketers
16 and questionable distribution of personal information
17 by on-line companies.
18 (10) In 1999, the Federal Trade Commission
19 found that 87 percent of Internet sites provided
20 some form of privacy notice, which represented an
21 increase from 15 percent in 1998.
22 (11) The United States is the leading economic
23 and social force in the global information economy,
24 largely because of a favorable regulatory climate and
25 the free flow of information. It is important for the

United States to continue that leadership. As nations and governing bodies around the world begin to establish privacy standards, these standards will directly affect the United States.

(12) The shift from an industry-focused economy to an information-focused economy calls for a reassessment of the most effective way to balance personal privacy and information use, keeping in mind the potential for unintended effects on technology development, innovation, the marketplace, and privacy needs.

SEC. 3. ESTABLISHMENT.

There is established a commission to be known as the ``Commission for the Comprehensive Study of Privacy Protection'' (in this Act referred to as the ``Commission'').

SEC. 4. DUTIES OF COMMISSION.

(a) STUDY.Ð The Commission shall conduct a study of issues relating to protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing appropriate uses of information, including the following:

(1) The monitoring, collection, and distribution of personal information by Federal, State, and local governments, including personal information col-

1 lected for a decennial census, and such personal in-
2 formation as a driver's license number.
3 (2) Current efforts to address the monitoring,
4 collection, and distribution of personal information
5 by Federal and State governments, individuals, or
6 entities, includingÐ
7 (A) existing statutes and regulations relat-
8 ing to the protection of individual privacy, such
9 as section 552a of title 5, United States Code
10 (commonly referred to as the Privacy Act of
11 1974) and section 552 of title 5, United States
12 Code (commonly referred to as the Freedom of
13 Information Act);
14 (B) legislation pending before the Con-
15 gress;
16 (C) privacy protection efforts undertaken
17 by the Federal Government, State governments,
18 foreign governments, and international gov-
19 erning bodies;
20 (D) privacy protection efforts undertaken
21 by the private sector; and
22 (E) self-regulatory efforts initiated by the
23 private sector to respond to privacy issues.
24 (3) The monitoring, collection, and distribution
25 of personal information by individuals or entities, in-

1 cluding access to and use of medical records, finan-
2 cial records (including credit cards, automated teller
3 machine cards, bank accounts, and Internet trans-
4 actions), personal information provided to on-line
5 sites accessible through the Internet, Social Security
6 numbers, insurance records, education records, and
7 driver's license numbers.
8 (b) FIELD HEARINGS.Ð
9 (1) IN GENERAL.Ð The Commission shall con-
10 duct at least four field hearings in each of the five
11 geographical regions of the United States.
12 (2) BOUNDARIES.Ð For purposes of this sub-
13 section, the Commission may determine the bound-
14 aries of the five geographical regions of the United
15 States.
16 (c) REPORT.Ð
17 (1) IN GENERAL.Ð Not later than 18 months
18 after appointment of all members of the
19 CommissionÐ
20 (A) a majority of the members of the Com-
21 mission shall approve a report; and
22 (B) the Commission shall submit the ap-
23 proved report to the Congress and the Presi-
24 dent.

1 (2) CONTENTS.—The report shall include a de-
2 tailed statement of findings, conclusions, and rec-
3 ommendations, including the following:
4 (A) Findings on potential threats posed to
5 individual privacy.
6 (B) Analysis of purposes for which sharing
7 of information is appropriate and beneficial to
8 consumers.
9 (C) Analysis of the effectiveness of existing
10 statutes, regulations, private sector self-regu-
11 latory efforts, technology advances, and market
12 forces in protecting individual privacy.
13 (D) Recommendations on whether addi-
14 tional legislation is necessary, and if so, specific
15 suggestions on proposals to reform or augment
16 current laws and regulations relating to indi-
17 vidual privacy.
18 (E) Analysis of purposes for which addi-
19 tional regulations may impose undue costs or
20 burdens, or cause unintended consequences in
21 other policy areas, such as security, law en-
22 forcement, medical research, or critical infra-
23 structure protection.
24 (F) Cost analysis of legislative or regu-
25 latory changes proposed in the report.

1 (G) Recommendations on non-legislative
2 solutions to individual privacy concerns, includ-
3 ing education, market-based measures, industry
4 best practices, and new technology.
5 (d) ADDITIONAL REPORT.Đ Together with the report
6 under subsection (c), the Commission shall submit to the
7 Congress and the President any additional report of dis-
8 senting opinions or minority views by a member of the
9 Commission.
10 (e) INTERIM REPORT.Đ The Commission may submit
11 to the Congress and the President an interim report ap-
12 proved by a majority of the members of the Commission.
13 **SEC. 5. MEMBERSHIP.**
14 (a) NUMBER AND APPOINTMENT.Đ The Commission
15 shall be composed of 17 members appointed as follows:
16 (1) 4 members appointed by the President.
17 (2) 4 members appointed by the majority leader
18 of the Senate.
19 (3) 2 members appointed by the minority leader
20 of the Senate.
21 (4) 4 members appointed by the Speaker of the
22 House of Representatives.
23 (5) 2 members appointed by the minority leader
24 of the House of Representatives.

1 (6) 1 member, who shall serve as Chairperson
2 of the Commission, appointed jointly by the Presi-
3 dent, the majority leader of the Senate, and the
4 Speaker of the House of Representatives.
5 (b) DATE OF APPOINTMENT.Ð The appointment of
6 the members of the Commission shall be made not later
7 than 30 days after the date of the enactment of this Act.
8 (c) TERMS.Ð Each member of the Commission shall
9 be appointed for the life of the Commission.
10 (d) VACANCIES.Ð A vacancy in the Commission shall
11 be filled in the same manner in which the original appoint-
12 ment was made.
13 (e) COMPENSATION; TRAVEL EXPENSES.Ð Members
14 of the Commission shall serve without pay, but shall re-
15 ceive travel expenses, including per diem in lieu of subsist-
16 ence, in accordance with sections 5702 and 5703 of title
17 5, United States Code.
18 (f) QUORUM.Ð A majority of the members of the
19 Commission shall constitute a quorum, but a lesser num-
20 ber may hold hearings.
21 (g) MEETINGS.Ð
22 (1) IN GENERAL.Ð The Commission shall meet
23 at the call of the Chairperson or a majority of its
24 members.

1 (2) INITIAL MEETING.—Not later than 45 days
2 after the date of the enactment of this Act, the
3 Commission shall hold its initial meeting.

4 **SEC. 6. DIRECTOR; STAFF; EXPERTS AND CONSULTANTS.**

5 (a) DIRECTOR.—
6 (1) IN GENERAL.—On or after October 1,
7 2000, the Commission shall appoint a Director with-
8 out regard to the provisions of title 5, United States
9 Code, governing appointments to the competitive
10 service.
11 (2) PAY.—The Director shall be paid at the
12 rate payable for level III of the Executive Schedule
13 established under section 5314 of such title.
14 (b) STAFF.—The Director may appoint staff as the
15 Director determines appropriate.
16 (c) APPLICABILITY OF CERTAIN CIVIL SERVICE
17 LAWS.—
18 (1) IN GENERAL.—The staff of the Commission
19 shall be appointed without regard to the provisions
20 of title 5, United States Code, governing appoint-
21 ments in the competitive service.
22 (2) PAY.—The staff of the Commission shall be
23 paid in accordance with the provisions of chapter 51
24 and subchapter III of chapter 53 of that title relat-
25 ing to classification and General Schedule pay rates,

1 but at rates not in excess of the maximum rate for
2 grade GS-15 of the General Schedule under section
3 5332 of that title.

4 (d) EXPERTS AND CONSULTANTS.—The Director
5 may procure temporary and intermittent services under
6 section 3109(b) of title 5, United States Code.

7 (e) STAFF OF FEDERAL AGENCIES.—

8 (1) IN GENERAL.—Upon request of the Direc-
9 tor, the head of any Federal department or agency
10 may detail, on a reimbursable basis, any of the per-
11 sonnel of that department or agency to the Commis-
12 sion to assist it in carrying out this Act.

13 (2) NOTIFICATION.—Before making a request
14 under this subsection, the Director shall give notice
15 of the request to each member of the Commission.

16 **SEC. 7. POWERS OF COMMISSION.**

17 (a) HEARINGS AND SESSIONS.—The Commission
18 may, for the purpose of carrying out this Act, hold hear-
19 ings, sit and act at times and places, take testimony, and
20 receive evidence as the Commission considers appropriate.
21 The Commission may administer oaths or affirmations to
22 witnesses appearing before it.

23 (b) POWERS OF MEMBERS AND AGENTS.—Any mem-
24 ber or agent of the Commission may, if authorized by the

1 Commission, take any action which the Commission is au-
2 thorized to take by this section.

3 (c) OBTAINING OFFICIAL DATA.Đ The Commission
4 may secure directly from any department or agency of the
5 United States information necessary to enable it to carry
6 out this Act. Upon request of the Chairperson of the Com-
7 mission, the head of that department or agency shall fur-
8 nish that information to the Commission.

9 (d) MAILS.Đ The Commission may use the United
10 States mails in the same manner and under the same con-
11 ditions as other departments and agencies of the United
12 States.

13 (e) ADMINISTRATIVE SUPPORT SERVICES.Đ Upon
14 the request of the Director, the Administrator of General
15 Services shall provide to the Commission, on a reimburs-
16 able basis, the administrative support services necessary
17 for the Commission to carry out this Act.

18 (f) GIFTS AND DONATIONS.Đ The Commission may
19 accept, use, and dispose of gifts or donations of services
20 or property to carry out this Act, but only to the extent
21 or in the amounts provided in advance in appropriation
22 Acts.

23 (g) CONTRACTS.Đ The Commission may contract
24 with and compensate persons and government agencies for

1 supplies and services, without regard to section 3709 of
2 the Revised Statutes (41 U.S.C. 5).

3 **SEC. 8. TERMINATION.**

4 The Commission shall terminate 30 days after sub-
5 mitting a report under section 4(c).

6 **SEC. 9. AUTHORIZATION OF APPROPRIATIONS.**

7 (a) IN GENERAL.Ð There are authorized to be appro-
8 priated to the Commission $2,500,000 to carry out this
9 Act.

10 (b) AVAILABILITY.Ð Any sums appropriated pursu-
11 ant to the authorization in subsection (a) shall remain
12 available until expended.

13 **SEC. 10. BUDGET ACT COMPLIANCE.**

14 Any new contract authority authorized by this Act
15 shall be effective only to the extent or in the amounts pro-
16 vided in advance in appropriation Acts.

○

Mr. HORN. At the subcommittee's first hearing on H.R. 4049, experts in the areas of medicine, finance, and Internet privacy shared their views on the many challenges involved in protecting privacy. Witnesses discussed their concerns about the increasing accessibility to personal information, such as medical records, Social Security numbers, and credit card records.

Both today and tomorrow, the subcommittee will continue this discussion with people knowledgeable in privacy issues.

I welcome our witnesses, and look forward to their testimony.

Let me just explain how the panels work. We will be swearing in all witnesses today. We would like you to summarize your statements. We have read all of them, and we would like you to do that in 5 minutes. So we will now finish with the opening statements, and I will give you the oath when those statements are through.

I now call on the gentleman from Texas, the ranking member, Mr. Turner, for his opening statement.

Mr. TURNER. Thank you, Mr. Chairman.

This is the second of three hearings that we have had scheduled on H.R. 4049, and I want to thank the chairman for prioritizing the need to study this very important issue. There is no doubt that privacy is one of the top concerns of the American people and one of the most important issues facing this Congress.

I am pleased to be a cosponsor of this legislation which would create a commission that will enable us to have a full and open discussion with the American people about privacy so we can address it in an appropriate manner. However, I do not want us to rush forward with the bill without proceeding cautiously and considering a number of issues surrounding the creation of this commission.

I commend Congressman Hutchinson for his leadership on this very important issue. At our first hearing, witnesses raised questions regarding the relationship the commission's work would have with privacy efforts by other entities. Specifically, concerns were voiced as to whether the commission could serve as a delay to regulations, studies that are currently moving forward. For example, witnesses pointed out that a bipartisan congressional privacy caucus is currently pushing for passage of a financial privacy measure.

Pursuant to the congressional mandate, the Secretary of HHS is now in the process of finalizing medical privacy regulations. Additionally, the Department of Treasury study on financial privacy regulations is soon to be completed.

We have many issues that need to be dealt with immediately, and I was pleased to hear Congressman Hutchinson state that the intent of the bill was not to impede the progress of other regulations which may reach consensus during the commission, rather, to be used as a sounding board to those initiatives.

Questions have arisen regarding the composition and expertise of members selected to the commission. Currently, the bill does not contain requirements regarding the qualifications of commission members. We need to ensure that an appropriate balance between all stakeholders in this issue is represented.

Witnesses also questioned the scope of the commission's mandate, which currently is not set forth in the bill. We should be concerned about duplicating work which has already been done and

consider whether it might be more productive for the commission to focus on specific privacy issues.

In light of the concerns that witnesses raised at the first hearing, members of the past and present entities charged with studying privacy issues as well as Federal and State government representatives who have been active on privacy matters have been identified and asked to testify before this subcommittee. These witnesses are expected to address the types of expertise and background that should be sought in the commission members, the types of issues that should receive focus and the types of reviews that may be redundant.

Again, I want to thank the chairman for holding the hearings; and I welcome the witnesses here today.

Mr. Waxman also advises me that he appreciates you scheduling the hearings to ensure that the issues raised by the legislation receive careful consideration. Mr. Waxman sends his regrets. He is unable to be here today, but he plans to attend tomorrow's hearing and looks forward to receiving the testimony from today's hearing.

The American people deserve to have their privacy protected in a correct and timely fashion. It is my hope that as a result of these hearings, we will be closer to that goal.

Thank you, Mr. Chairman.

Mr. HORN. We thank you. And now we have a member of the full committee who is the author of the legislation, the gentleman from Arkansas, Mr. Hutchinson, for an opening statement.

Mr. HUTCHINSON. I thank the chairman, and I just want to take a moment to express my appreciation to you and the committee for scheduling a second day of hearings.

During the last break, I believe it was, I received a copy of a letter from Mr. Waxman requesting additional hearings; and as one of the lead sponsors of this legislation I was delighted of his interest in it; and I appreciate the chairman scheduling this hearing so promptly to followup on Mr. Waxman's request.

I also appreciate Mr. Turner, the ranking member, and his leadership on this issue which has been critical from the very beginning. It has been a goal to make sure that this is—privacy is pursued in a bipartisan fashion, and the participation of Mr. Turner and the many Democrats who have joined on this legislation is important to its success and ultimate credibility.

Mr. Turner outlined a number of concerns—I wouldn't say a number. There were serious concerns raised in the last hearing that are very legitimate in terms of we should discuss those and perhaps look at amending the legislation, if necessary, as we go through the markup process. It is certainly not the intent of the privacy commission to serve as a delay on other legitimate efforts to address privacy concerns. I have always viewed this as complementary. Whatever happens in other arenas on a smaller scale, it is important to look at privacy in a comprehensive way and in an ongoing way.

Second, it was discussed about the diversity of the commission members, and certainly I believe that the point of authority should seek to ensure that membership of the commission will represent a diversity of views and experiences on the issues that they will address in terms of privacy, and that is important.

So we are happy to work with those who are supportive of privacy—of the privacy commission to make sure that it is drafted in a fair manner and move this ball forward and protect privacy in a balanced way.

Mr. Chairman, I thank you; and I look forward to the testimony of the witnesses.

Mr. HORN. I thank the gentleman.

Now if the witnesses will stand.

[Witnesses sworn.]

Mr. HORN. The clerk will note that there are five witnesses that accepted the oath.

The Honorable John Spotila is the Administrator of the Office of Regulatory Affairs in the Office of Management and Budget. Mr. Spotila.

STATEMENT OF JOHN SPOTILA, ADMINISTRATOR, OFFICE OF REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Mr. SPOTILA. Mr. Chairman and members of the committee, thank you for inviting me here to present the administration's views on H.R. 4049, the Privacy Commission Act.

As Administrator of OMB's Office of Information and Regulatory Affairs, I care deeply about the protection of privacy. In 1998, OIRA took on enhanced responsibility for coordinating privacy policy throughout the administration. OIRA already had policy responsibility under the Privacy Act of 1974 which applies to Federal Government systems of records. Now it plays a central coordinating role for privacy policy more generally.

Last year OMB appointed its first Chief Counselor for Privacy, Peter Swire, to be the point person in this coordination effort; and Peter is here with me today and available if needed.

The President and the Vice President are committed to the protection of individual privacy. As President Clinton said on April 30 when announcing his new financial privacy proposal, "From our earliest days, part of what has made America unique has been our dedication to freedom and the clear understanding that real freedom requires a certain space of personal privacy."

In studying the proposed findings for H.R. 4049, we find much common ground. We agree that Americans are increasingly concerned about the security and use of their personal information. We agree that the shift from an industry-focused economy to an information-focused economy calls for reassessing the way we balance personal privacy and information use.

As Administrator of OIRA, I work extensively on information policy issues relating to computer security, privacy, information collection, and our transition to the electronic delivery of government services. In these and other areas, we are working hard to gain the advantages that come from new technologies while guarding against possible costs to privacy and security that can come from badly crafted uses of those technologies.

In some areas, we already know that we must act swiftly to protect privacy and security. Indeed, the administration's biggest concern with H.R. 4049 is the risk that you highlighted earlier, the risk that some might use the commission as a reason to delay

much-needed privacy legislation. We understand that supporters of H.R. 4049 have emphasized that it should not be used as a reason for delay, and we agree with that, but we are concerned that there are those that would oppose privacy reform who would prefer to have Congress study the issue indefinitely rather than take action. We cannot afford to take a year and a half off in protecting Americans' privacy. We believe that action is needed now in the areas of financial privacy, medical records privacy, and genetic discrimination.

There have been extensive initiatives by the Federal Government since 1993 to study and take appropriate action in the area of privacy protection. Study of privacy was an integral part of the National Information Infrastructure project, sometimes called the "information superhighway" effort, with the issuance in 1995 by an interagency privacy working group of principles for providing and using personal information. This effort was led by OIRA—before I was there, I will admit.

With the administration's support, Congress has passed a long list of privacy legislation. In my written statement, we provide details about these laws and other activities by the administration to protect Americans' privacy.

My statement also explains the legislation that is now before the Congress to provide legal protections for three especially sensitive categories of personal information: financial records, medical records, and genetic discrimination.

Let me turn again to the specifics of H.R. 4049.

The administration does have concerns that the study commission might be used as an excuse for delaying needed activity in privacy protection, and we appreciate the strong statements we heard today that indicate that you agree that should not happen. These concerns would be especially acute for these important topics such as medical, financial, and genetic information. We know there has already been extensive discussion of these proposals, and we would not want to see further study duplicating the public examination that has already taken place without adding real value.

We recognize that the Congress needs to make its own judgments on these matters, and we defer to it in its assessment of what it needs to inform those judgments. It seems sensible, however, to adopt a focused approach to exploring these topics. Ideally, any further study efforts should be done within a short timeframe and would build on, not duplicate, existing studies.

If there were to be a commission, we should ensure that it focuses its efforts in an effective way. Casting too broad a net would delay the work of any new commission, with uncertain results. We note, for example, that the treatment of data collected on-line has been the subject of extensive hearings in Congress as well as public workshops, public comments, studies, and reports. The Federal Trade Commission is about to issue a major report. We recognize that this is a complicated area that requires careful evaluation and an understanding of new technology. It is not clear, however, that a commission lasting 18 months will give decisionmakers the help they need in this area.

Rather than have a commission pursuing a very broad set of topics, it might be more productive to have technology and policy ex-

perts address specific, emerging issues that have not yet benefited from much attention. One targeted way to study such issues might be to enlist the expertise of the National Academy of Sciences/National Research Council, which has already produced studies in areas such as cryptography and medical records privacy. We could call it in again on emerging areas of concern. These might be particularly appropriate for examining authentication technologies and their privacy implications and the topic of biometrics and privacy.

For all of these reasons, we believe that there may be sound alternatives to a privacy commission. If legislation creating a commission does move forward, however, we do have some specific concerns about the method of appointment of commissioners, and the possibility that the current draft could lead to the release of classified information.

We share with Congress a very strong interest in protecting privacy. We look forward to working with you to find suitable new ways to improve that protection. We understand the good intentions motivating the sponsors of H.R. 4049; and, despite our reservations about the specifics of this bill, we welcome the commitment to privacy protection that they seek to demonstrate.

Thank you once again for the invitation to discuss these issues.

Mr. HORN. We thank you for that very concise presentation.

[The prepared statement of Mr. Spotila follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Spotila

STATEMENT OF

JOHN T. SPOTILA

ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET

SUBMITTED TO

THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

MAY 15, 2000

Mr. Chairman and members of the Committee, thank you for inviting me here to present the Administration's views on H.R. 4049, the "Privacy Commission Act." As Administrator of OMB's Office of Information and Regulatory Affairs, I care deeply about the protection of privacy. In 1998, OIRA took on enhanced responsibility for coordinating privacy policy throughout the Administration. OIRA already had policy responsibility under the Privacy Act of 1974, which applies to federal government systems of records. Now it plays a cental coordinating role for privacy policy more generally. Last year, OMB appointed its first Chief Counselor for Privacy, Peter Swire, to be the point person in this coordination effort. Peter is with me here today.

The President and the Vice President are committed to the protection of individual privacy. As President Clinton said on April 30, when announcing his new financial privacy proposal: "From our earliest days, part of what has made America unique has been our dedication to freedom, and the clear understanding that real freedom requires a certain space of personal privacy." Vice President Gore showed similar leadership in 1998 when he called for an Electronic Bill of Rights, emphasizing that we should all do our part to protect individual privacy, relying on private sector leadership where possible, on legislation when necessary, on responsible government handling of personal information, and on an informed public.

In studying the proposed findings for H.R. 4049, we find much common ground. We agree that Americans are increasingly concerned about the security and use of their personal

information. We agree that the shift from an industry-focused economy to an information-focused economy calls for reassessing the way we balance personal privacy and information use. As Administrator of OIRA, I work extensively on information policy issues relating to computer security, privacy, information collection, and our transition to the electronic delivery of government services. In these and other areas, we are working hard to gain the advantages that come from new technologies while guarding against possible costs to privacy and security that can come from badly crafted uses of those technologies.

In some areas, we already know that we must act swiftly to protect privacy and security. Indeed, the Administration's biggest concern with H.R. 4049 is the risk that some might use the Commission as a reason to delay much-needed privacy legislation. We understand that supporters of H.R. 4049 have emphasized that it should not be used as a reason for delay. But we are also aware from public reports that those who oppose privacy reform would prefer to have Congress study the issue indefinitely rather than take action. In the Administration's view, such delay would be unwise. We cannot afford to take a year and a half off in protecting Americans' privacy. We believe that action is needed now in the areas of financial privacy, medical records privacy, and genetic discrimination.

Before addressing specific aspects of H.R. 4049, it would be useful to review recent federal privacy initiatives.

Overview

There have been extensive initiatives by the Federal government since 1993 to study and take appropriate action in the area of privacy protection. Study of privacy was an integral part of the National Information Infrastructure project, sometimes called the "information superhighway" effort, with the issuance in 1995 by an inter-agency Privacy Working Group of "Principles for Providing and Using Personal Information." (See: Privacy Working Group of the Information Infrastructure Task Force, www.iitf.nist.gov/ipc/ipc-pub.html.) This effort was led by OIRA. With Administration support, Congress has passed privacy legislation including the Drivers' Privacy Protection Act of 1994 (motor vehicle records), the Telecommunications Act of 1996 (authority for the Customer Proprietary Network Information regulations), the Health Insurance Portability and Accountability Act of 1996 (authority for the currently proposed medical privacy regulations), the Children's Online Privacy Protection Act of 1998 (children's online records), the Identify Theft and Assumption Deterrence Act of 1998 (deterrence of identity theft), and the Gramm-Leach-Bliley Act of 1999 (financial records).

In the online world, the Administration has encouraged self-regulatory efforts by industry. For especially sensitive information -- such as medical, financial, and children's online records -- legal protections are required. Recent activities have included:

- When children go online, parents should give their consent before companies gather personal information. Websites aimed at children must get such consent

under the Children's Online Privacy Protection Act of 1998 and accompanying rules that went into effect in April of this year.

- The Department of Commerce, the Federal Trade Commission, the White House Electronic Commerce Working Group, and other parts of the Federal government have undertaken a wide array of studies, reports, workshops, and other activities to address issues of online privacy. As one example, a public workshop last fall challenged the industry to address concerns about "online profiling," in which companies collect data, in ways few people would suspect, about individuals surfing the Internet.

- In the international sphere, the Department of Commerce has taken the lead in creating "safe harbor" principles for transfers of personal information between the European Union and the United States. These principles, to which the European Commission has now agreed, recognize the appropriateness of effective self-regulatory regimes. In developing the principles, the Department has sought public comment on four separate occasions.

- The President signed the Identity Theft and Assumption Deterrence Act of 1998. This March, the Department of the Treasury hosted an Identity Theft Summit to assist in the prevention, detection, and remediation of the significant problem of malicious misuse of another person's personal information for fraudulent purposes.

- The Administration continues to build privacy protections into its own activities. Last year, for instance, all Federal agencies successfully posted clear privacy policies on their websites. Programs are now underway to strengthen Government computer security to provide new privacy safeguards for personal information held by the Government. The new Privacy Subcommittee of the Chief Information Officers Council is undertaking initiatives to ensure that privacy is effectively built into government information technology systems.

Financial records.

Congress discussed financial privacy intensively in the course of its financial modernization debate last year. As the President pointed out when signing the law, the modernization law took significant steps to protect the privacy of financial transactions, but did not go far enough. The President asked OMB, the Department of Treasury, and the National Economic Council to craft a legislative proposal to close loopholes under existing law. On April 30, he announced his plan to protect consumers' financial privacy. This plan would include:

- Consumer choice: Giving consumers the right to choose whether a firm can share consumer financial information with third parties or affiliated firms.

- Enhanced protection for especially sensitive information: Requiring that a consumer give affirmative consent before a firm can gain access to medical information within the financial conglomerate, or share detailed information about a consumer's personal spending habits.

- Access and correction: Giving consumers a new right to review their information and correct material errors.

- Effective enforcement: Providing effective enforcement tools for financial institutions subject to Federal Trade Commission enforcement of privacy rules.

- Comparison shop on privacy policies: Giving consumers privacy notices upon application or request so they know how information is protected before a customer relationship is established.

These provisions were introduced in the House as H.R. 4380, attracting immediate and substantial support in both the House and the Senate. As Secretary of the Treasury Lawrence Summers emphasized on March 7, "It's time to start now."

Medical Records.

There has been a longstanding appreciation in the United States that individual medical records include especially sensitive information. Disclosing medical data can reveal what is happening inside a person's body, such as a report that a person is HIV positive, or inside a person's mind, such as the transcript of a session with a psychotherapist. The Federal government has recognized these concerns at least since 1973, when the Department of Health, Education, and Welfare first announced the basic fair information practices that underlie privacy policy today.

Congress recognized the need for legal protection of medical records when it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). After extensive discussions with stakeholders and as required by HIPAA, the Secretary of Health and Human Services issued her recommendations for health privacy legislation in September 1997. Congress was unable to meet the HIPAA deadline for enacting comprehensive privacy legislation by August 21, 1999. Accordingly, the President and Secretary Shalala announced proposed privacy regulations on October 29 of last year. It was HHS's goal to make the regulation process open to those who wanted to communicate their concerns in person. HHS met with many individuals and organizations to hear their concerns and clarify provisions of the proposed rule. HHS received over 53,000 submissions of comments by the February 17, 2000 deadline. HHS is now considering those comments, and the regulations will become final this year.

Although the medical privacy regulations will become final this year, there is a pressing need for further Congressional action. As HHS Assistant Secretary Margaret Hamburg testified in February of this year: "Health information privacy is a top priority for the Department and the Administration, and we continue to believe that legislation is the only way to achieve the goal." President Clinton explained some of the reasons for legislation when he proposed the privacy regulations last October. The Administration is especially concerned that the enforcement powers under current law are not as effective as they should be. We recommend federal legislation that would allow punishment of those who misuse personal health information and redress for people who are harmed by its misuse. Administration officials have testified often on what should be included in medical privacy legislation, and we urge that there be no delay on this subject.

Genetic Discrimination.

This February 8, President Clinton signed an executive order that prohibits every federal department and agency from using genetic information in any hiring or promotion action. This order ensures that critical health information from genetic tests not be used against federal employees. The President has also endorsed the Genetic Nondiscrimination in Health Insurance and Employment Act of 1999, introduced by Senator Daschle and Congresswoman Slaughter, which would extend these protections to the private sector and to individuals purchasing health insurance. As with financial and medical privacy, legislation is before the Congress to address especially sensitive personal data -- genetic information on individuals. The time to act on each of these issues is now.

* * * *

Let me turn now to the specifics of H.R. 4049.

The Scope and Structure of the Proposed Commission.

As indicated earlier, the Administration has significant concerns that the Study Commission might be used by some as an excuse for delaying needed activity in privacy protection. These concerns are especially acute for topics such as medical, financial, and genetic information where good legislative proposals are before the Congress now. There has already been extensive discussion of these proposals within the Congress and among the stakeholders. Further study of these topics by the Commission would duplicate the public examination that has already taken place, without adding real value. The proposed medical privacy rules that become final this year will be the result of a multi-year process that generated over 53,000 public comments, many in extensive detail. These comments show a need for further action, not further study.

We recognize that the Congress needs to make its own judgments on these matters, and we defer to it in its assessment of what it needs to inform those judgments. It seems sensible, however, to adopt a focused approach to exploring these topics. Ideally, any further study efforts

should be done within a short time frame and would build on, not duplicate, existing studies.

If there were to be a Commission, contrary to our recommendation, we should ensure that it focuses its efforts in an effective way. Again, we are concerned about potential delay. Casting too broad a net would delay the work of any new Commission, with uncertain results. We note, for example, that the treatment of data collected on-line has been the subject of extensive hearings in Congress, as well as public workshops, public comments, studies, and reports by the Department of Commerce and the White House Electronic Commerce Working Group. The Federal Trade Commission is about to issue a major report. We recognize that this is a complicated area that requires careful evaluation and an understanding of new technology. It is not clear, however, that a Commission lasting 18 months will give decisionmakers the help they need.

Indeed, rather than have a Commission pursuing a very broad set of topics, it might be more productive to have technology and policy experts address specific, emerging issues that have not yet benefitted from much attention. One targeted way to study such privacy issues might be to enlist the expertise of the National Academy of Sciences/National Research Council or other appropriate bodies. The NAS/NRC has extensive experience in creating blue-ribbon groups with the expertise to provide insight into difficult policy problems. In the privacy area, the NAS/NRC has already produced studies such as "Cryptography's Role in Securing the Information Society" (1996) and "For the Record: Protecting Electronic Health Information" (1997). Perhaps we should call on it again.

The NAS/NRC's Computer Science and Telecommunications Board is currently exploring funding for a study on "Authentication Technologies and Their Privacy Implications." The problem identified for this study arises from the need to identify people in a trustworthy way–that is, to authenticate people–in order to facilitate business and other activities over the Internet. Many of the possible ways to identify people have privacy implications since they involve individuals turning over a good deal of personal information -- from a mother's maiden name to credit card numbers or other information that could put an individual at risk if revealed to unauthorized persons. As technology develops, our society needs to understand how to make authentication work in a way consistent with preserving privacy.

Another useful study topic, which similarly does not require a Commission, could be biometrics and privacy. "Biometrics" refer to fingerprints, iris scans, and other physical indicators of identity. Since many companies are now exploring the commercial deployment of biometric technology, now is a good time to assess the public policy of biometrics and privacy. If deployed carefully, biometrics could protect privacy by placing less reliance on sending credit card numbers or other sensitive information over the Internet. If deployed badly, however, biometric technology could create new privacy risks, such as if biometrics were used to record each room an employee enters while on the job. A study of this subject, taking proper account of new technological developments, could increase the likelihood that biometric systems will be more sensitive to privacy concerns as they become widely used.

For all these reasons, we believe there are sound alternatives to a Privacy Commission. If, nonetheless, legislation creating such a Commission moves forward, then we have specific concerns about certain provisions in H.R. 4049. For instance, as with other commissions on many important national issues, the President should have a greater role in appointing Commission members. In addition, the current section 7(c) is objectionable because it could be interpreted as requiring Executive Branch agencies to turn over confidential or classified information to the proposed Commission. The text could read that agencies "may," rather than "shall" furnish that information.

As I emphasized earlier, we share with the Congress a very strong interest in protecting privacy and look forward to working with you to find suitable new ways to improve that protection. We understand the good intentions motivating the Congressional sponsors of H.R. 4049. Despite our reservations about the specifics of this bill, we welcome the commitment to privacy protection that they seek to demonstrate.

Mr. Chairman and Members of the Committee, thank you once again for the invitation to discuss these issues.

Mr. HORN. Our next presenter is David Veator, who is with the Office of Consumer Affairs and Business Regulation for the State of Massachusetts. Mr. Veator.

STATEMENT OF DAVID VEATOR, OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, STATE OF MASSACHUSETTS

Mr. VEATOR. Thank you, Mr. Chairman and members of the committee. My name is David Veator, and I am the general counsel for the Massachusetts Office of Consumer Affairs and Business Regulation. Our office is charged with the oversight of all State-chartered banks, insurance companies, most of the professional trades and the supervision of the State's consumer protection laws.

Because issues of privacy are of growing importance both to consumers and the businesses that my agency regulates, our agency is the one in Massachusetts that has been tapped with supporting Governor Cellucci and Lieutenant Governor Swift's privacy agenda, and on behalf of them, I am pleased to testify in support of the privacy commission proposed in H.R. 4049.

As this committee knows, privacy issues are now at the forefront of the national discourse. As we say in our prepared statement, the information age has brought many good things to people, but no silver lining is without its cloud. With the rapid growth in technology to collect and compile personal information, citizens face unprecedented threats to their personal privacy. One recent poll conducted by Lou Harris & Associates noted that 88 percent of Americans are concerned about threats to personal privacy and that 83 percent believe that consumers have lost all control over how companies collect and use their personal information.

For a small fee there are companies that can collect more information than you would have believed about you and compile it and disseminate it, and one of the witnesses in this committee's last hearing demonstrated that in some detail.

I am sure that each of the members of this committee is aware that this widespread perception of privacy abuse has already translated into action at the State and Federal level. Although this action has resulted in good legislation and improving industry practices, it is fair to say that our approach to privacy is disjointed and ad hoc. According to several commentators, between 2,000 and 3,000 privacy-related bills are currently pending in State legislatures. Many of these bills deal with multiple privacy issues. It would appear that this less-than-coordinated approach to privacy cannot be an efficient way to deal with the subject.

Another problem with our approach to privacy to date has been a criticism that it is too sectorial, that is, different legislation tends to tackle privacy issues with respect to different industries. As a result, we have on-line privacy rules, privacy rules for brick and mortar companies, banking privacy rules, insurance privacy rules, and telecommunications privacy rules. Privacy in American Business reported that, by the end of 1999, 179 different privacy laws relating to health care had been enacted, as had 65 privacy laws related to direct marketing or telecommunications, 59 relating to financial services, 39 relating to insurance and 14 relating to on-line or Internet activity.

This approach may have been workable in the past, but as the nature of our economy changes it may no longer make sense. For example, as the financial services industry has revolutionized and converged, several isolated privacy statutes that deal with banking or insurance or securities may no longer have much application.

We think that the commission proposed by Congressmen Hutchinson and Moran is a logical way to approach the question of privacy. There are obvious advantages to taking a comprehensive look at the array of complex privacy issues such as financial privacy, identity theft, biometrics and children's privacy, etc.

The most obvious benefits are the ability to take advantage of work that has been done both at the Federal level and at the various States and take advantage of nationwide expertise. I would like to offer the experience of Massachusetts.

Shortly after their election, Governor Cellucci and Lieutenant Governor Swift convened a working group to examine the quality of life in Massachusetts. We were able to consult with privacy experts, local business leaders, and law enforcement, and shortly thereafter Governor Cellucci and Lieutenant Governor Swift filed a comprehensive bill on privacy that updated existing privacy laws to reflect the technological changes that have occurred since their inception and instituted new protections to address new technology. The intent of the bill was to empower consumers in the 21st century economy while continuing to allow Massachusetts business to flourish.

I can also point to the experience of the FTC Subcommittee on Access and Security which recently reported to the FTC, and the FTC I think was able to develop a committee that provided a robust analysis precisely because it had many viewpoints from across the country on that committee.

I would like to close by saying a few words about one State's view of the roles of both Federal and State examination of privacy.

I think the States will continue to legislate and act to protect their citizens, but we believe that the Congress has a unique capacity to develop workable privacy protections. It may be that most States would prefer not to act unilaterally if we were assured that the Federal Government and private industry are striking the right balance between the need of businesses for information and the right of citizens to personal privacy.

Indeed, a uniform approach to privacy confers two advantages from a State's point of view. It makes interstate commerce easier for businesses which only have to follow one set of rules rather than 50, and by establishing at least baseline standards for all States means that no State will have to potentially disadvantage its own economy by establishing on its own minimum protections for its own consumers.

In closing, I would like to thank the committee on behalf of Governor Cellucci and Lieutenant Governor Swift for this opportunity to testify. We support H.R. 4049 as a means for taking, for the first time, a national approach to privacy in a new economy. As I indicated, our economy has undergone a technological revolution, and the way in which privacy catches up to this revolution will have important consequences for us as individuals and for our new economy.

Thank you.

Mr. HORN. Well, we thank you. That is very helpful testimony, and we always appreciate it from the State of Massachusetts. You are usually ahead of the rest of the country quite a bit.

[The prepared statement of Mr. Veator follows:]

Veator

David L. Veator, General Counsel
Massachusetts Office of Consumer Affairs and Business Regulation
Testimony on HR 4049:
A Bill to Establish the Commission for the Comprehensive Study of Privacy Protection
before the House Committee on Government Reform
Monday, May 15, 2000

Chairman Burton and members of the committee, thank you for the opportunity to testify today. My name is David Veator and I am the General Counsel for the Massachusetts Office of Consumer Affairs and Business Regulation. My office is charged with the oversight of all state-chartered banks, insurance companies, most of the professional trades, and supervision of the state's consumer protection laws. Because issues of privacy are such a big concern to consumers and the businesses that my agency regulates, the Office of Consumers and Business Regulation is primarily responsible for pursuing the privacy agenda of Massachusetts Governor Paul Cellucci and Lieutenant Governor Jane Swift. On behalf of Governor Cellucci and Lieutenant Governor Swift, I am pleased to testify in support of the privacy commission proposed in House Bill 4049.

Privacy issues are now at the forefront in the national discourse. With the rapid growth in new technology to collect and compile personal information, citizens face unprecedented threats to their personal privacy. A recent poll conducted by Lou Harris & Associates noted that 88% of Americans are "concerned about threats to personal privacy" and that 83% believe that "consumers have lost all control" over how companies collect and use their personal information. The states and Congress are now being called upon by their citizens to protect privacy against these new threats.

The information age has brought many good things to many people. However, no silver lining is without its cloud. I believe that the privacy commission proposed by Congressmen Hutchinson and Moran could be a very important tool for us to address an ever-darkening cloud that the information age has brought us: an explosion of personal information about all of us, much of it easily accessible without our ever knowing who has it and who is asking for it. For a small fee, it is now possible to obtain intimate details about almost anyone from the comfort of your personal computer. The firms that provide this information are accountable to no one, and, for the most part, we have no right even to review the information in their files, much less require them to

correct erroneous information or delete overly personal details. This situation has made identity theft one of today's fastest growing crimes.

The growing threat to personal privacy is an issue of paramount importance not only to most residents in my home state Massachusetts, but to all Americans. It affects all of us, whether we realize it or not.

Although the states do have and should have a role in protecting the privacy of their citizens, we believe that Congress has a unique capacity to develop workable privacy protections. Business friendly states, such as Massachusetts, welcome national efforts by industry to protect privacy. Many responsible companies have committed a great deal of time and resources to enhance the privacy of their customers through their own initiatives and through self-regulatory organizations. Congress has recently also worked to ensure that privacy protections are in place for all Americans, not just Americans in some privacy conscious states. I believe that most states would prefer not to act unilaterally if they are assured that the federal government and industry are striking the right balance between the need of businesses for information and the right of citizens to their personal privacy. Indeed, states might legitimately fear that they may hurt their state economies if they alone pass laws or regulations viewed as too burdensome by businesses. While federal action by industry and government is preferable, states will act if they believe that their citizens privacy rights are not protected. As proof, the organization Internet Alliance estimates that more than 2,000 pieces of legislation have been filed regarding Internet-related issues alone.

By taking a comprehensive approach to the issue of privacy and involving interested parties across the nation, the privacy commission proposed by Congressmen Hutchinson and Moran could find an optimum balance. Both consumers and businesses would benefit from a shared consensus as to what are the best information practices.

Because of the flexibility in the proposed statute, the commission could focus energy on any issue where action is expected or even underway. For example, the commission could take up financial privacy issues that have been raised during the debate about the financial privacy regulations promulgated pursuant to the Graham-Leach-Bliley Act. Congress could benefit from ability of this commission to solicit views across America on these timely issues. Moreover, this commission could also help compile information from places where debate on these issues is already occurring.

There are distinct advantages to taking a comprehensive approach to privacy issues, such as financial privacy, identity theft, medical privacy, biometrics, children's privacy, etc. Two years ago, Massachusetts convened a working group of public and private sector leaders to do so. It found that although privacy is now a much bigger issue because of the speed at which electronic networks can disseminate it, many of these same privacy issues have been around for a long time in the off-line world. Many on-line businesses have raised the question why they are being singled out. Fair information practices should not only be an Internet concern, they should be a concern to all businesses. While different sectors of the economy may indeed have to treat information differently, there are baseline standards by which all business should abide, including hospitals, banks, and insurance companies.

Little detail about Mass experience. Omnibus legislation. Many different business representatives. Learned a great deal about how any government proposals could effect business processes. Many theories about how to govern e-commerce, from self-regulation to government rules. One theory is a mixing of all of them. Government could apply or enforce the base floor (where everyone is in agreement) and allow the market to develop around issues that are extremely contentious.

Little about FTC Conference - learned about issues before a law was being proposed.

Mr. HORN. Our next presenter is from another very progressive State and that is the State of Minnesota. We have the Attorney General from the State of Minnesota, Mike Hatch.

STATEMENT OF MIKE HATCH, MINNESOTA STATE ATTORNEY GENERAL

Mr. HATCH. Mr. Chairman and members of the committee, I have read the testimony that was presented at your prior hearing, and it is apparent that you have full grasp of this issue. You have examples of everything from perpetrators on the Internet taking photos out of yearbooks and putting them on pornography, displaying them out for the public. You have corporations asking self-insured administrators and even the government to draw profiles of their employees' health care and health conditions. You have telemarketing companies using bank data to target senior citizens, perpetrating financial fraud far beyond what was contemplated by enactment of the Vulnerable Adult Act.

It is very plain that something ought to be done now by policymakers. My concern with regard to a commission and with all due respect for studying it, this is an issue that is the result of technology, but it is not the issue of technology itself. It can be addressed and ought to be addressed, and all too often in our society—and I am afraid that is the case here—commissions or task forces are appointed to delay, to try to escape an issue.

Last year, Congress passed the Financial Services Modernization Act, and they lifted the Pandora's lid on privacy. They basically permitted banks to exchange information which under State law in most States fiduciary obligations would have prevented them or left them open to litigation for doing so. By opening that Pandora's lid, the playing field has changed so that now those institutions don't want to change. They have got it. Yet the public, by margins that were pointed out in poll after poll by the prior speaker, 85 percent strongly believe that action ought to be taken now.

Congress lifted the lid last year. It ought to put the lid back on—and I am talking about financial privacy, health care, the Internet—and start addressing the issue. Don't study it, but move on it.

Now, at the State level, we have several bills. We have gotten them through the Senate, and we are hopeful that we can get some bills through the House on this. We had over 100 lobbyists representing, according to the chairman of the Commerce Committee in the House, 59 interests at one hearing, which is considerable for a State legislature. They are all opposed to any change, and what their cry was, "leave it to Congress. Congress will change it. It is a Federal issue." And you know what is going to happen. You pass a bill having a commission, all 59 will be back. Let this commission come back.

But every day that we delay we have another stakeholder on this privacy issue. More data is exchanged about each of us. More privacy is invaded, more stakeholders and more lobbying techniques will follow. It is important. It is an important issue. People feel strongly about it. If a privacy commission were established where something was stated very clearly that the States should move forward now, that Congress should move forward now, that would be one thing. But it is extremely important—I don't think we have

done very much on this issue, contrary to perhaps some of the other speakers here, and I think the time is now for policymakers to stand up and have the courage to take on these interests and start enacting some legislation.

Mr. HORN. I thank you very much for your presentation. You can probably look around behind you and see a lot of interest there, too.

[The prepared statement of Mr. Hatch follows:]

STATE OF MINNESOTA

OFFICE OF THE ATTORNEY GENERAL

Hatch

MIKE HATCH
ATTORNEY GENERAL

102 STATE CAPITOL
ST. PAUL, MN 55155-1002
TELEPHONE: (651) 296-6196

May 15, 2000

Committee on Government Reform
Subcommittee on Government Management,
Information and Technology
United States House of Representatives
Washington, DC 20515

Re: Statement on H.R. 4049

Dear Committee Members:

I am the Attorney General for the State of Minnesota. I thank you for giving me this opportunity to respond to your request for input on H.R. 4049, the "Privacy Commission Act."

Minnesota Law Enforcement and Legislative Efforts

Our Office has worked hard to safeguard the privacy of Minnesotans both through law enforcement and legislative initiatives. On the law enforcement front, we were the first state to bring a one-two punch of financial privacy lawsuits--first against U.S. Bank for disclosing private financial information of their customers and then against MemberWorks, Inc., which used that information to telemarket its membership programs.

In our lawsuit against U.S. Bank, we alleged that the bank disclosed the names, phone numbers, social security numbers, account balances and credit limits of almost one million of its customers after telling its customers that "all personal information you supply to us will be considered confidential." The bank settled the case by agreeing not to disclose private information to non-affiliated third parties for purposes of marketing non-financial products and services. As a result, U.S. Bank is now ahead of many of the large national banks for respecting customer privacy. Unfortunately, a multitude of financial institutions throughout the country continue to violate their customers' trust by disclosing private information with outside telemarketers. What is even more unfortunate is that the recently-enacted federal Gramm-Leach-Bliley legislation does nothing but encourage this sort of activity.

As mentioned above, our state also filed suit against MemberWorks, which uses customer information obtained from financial institutions to market enrollment in membership programs offering discounts on such things as leisure apparel, videogames and computer software. MemberWorks used this data to telephone Minnesotans to offer a 30-day free trial enrollment in the membership programs, telling some consumers that "you don't have to make a decision over the phone." However, consumers actually were making an important decision over the phone – to allow MemberWorks to charge their credit card or checking account for enrollment in the membership club if the consumer did not call MemberWorks within 30 days to cancel. Numerous consumers believed they were protected because they had not revealed their account number to MemberWorks. Unfortunately, they did not know that MemberWorks in many cases had already obtained information about them from their financial institutions. MemberWorks made much fanfare about its claim that it had audiotapes documenting consumers' consent to such charges; however, many audiotapes produced by MemberWorks during our litigation did not document a meaningful consent from consumers prior to charging their accounts. Attached are two examples of scripts from our lawsuit.

This form of telemarketing is only possible when private information is disclosed by businesses, including banks, without the consent of consumers.

Although much of the discussion regarding financial privacy has focused upon non-affiliated third party sharing of financial information, our Office routinely receives complaints about the sharing of nonpublic personal information among affiliates. For example, a consumer recently complained that a large bank notified its securities affiliate of her account status. The securities affiliate then called the 85-year-old consumer and sold her a high-risk security that she was led to believe was a certificate of deposit. This sale would not have occurred but for the sharing of information among affiliates.

As a result of these and similar privacy invasions, many of them targeted against the elderly, we have pushed hard for privacy legislation in Minnesota. For instance, our Office supported legislation this session to strengthen the weak privacy protections in the Gramm-Leach-Bliley Act by requiring financial institutions to get written consent from their customers **before** disclosing their financial information to non-affiliates such as telemarketers. This is called an "opt in" system because it gives consumers the right to weigh in–to say "yes"–before their information is shared, compared to an "opt out" system which allows unlimited sharing of private information unless a consumer says "stop."

We included an "opt in" requirement in our privacy bills because citizens deserve choice and control over how their personal, sensitive, confidential information is used. An "opt in" system is not only most consistent with consumers' reasonable expectations, but is overwhelmingly favored by the public over an "opt out" system which simply sanctions rampant trafficking in information that should remain private until citizens say otherwise.

Privacy Commission Act, H.R. 4049

H.R. 4049 proposes to create a 17 member, $2.5 million federal privacy commission to simply study an issue that we, in the states, are already taking action on. With all due respect, further study is not the proper course, given the volume of ink already spilled on the privacy subject as well as the volume of consumer outcry--and violations--we hear in our daily work in the states.

First, a federal privacy commission will simply serve as yet another **excuse to delay** substantive enforcement and legislative action both at the federal and state levels.

Second, a privacy commission is unnecessary. Privacy has been frequently studied over the past several decades by the federal government, academia, non-profits, and even the private sector. The issue of privacy is one of policy, not science. H.R. 4049 will cost taxpayers $2.5 million to find out **what everyone already knows**--that companies collect a lot of information and disclose it without our knowledge or meaningful consent and that the public wants action.

Third, I cannot stress enough that your constituents want **real** privacy protections **now**, not another **study** of privacy protections for the next year and a half. Consumers are outspoken that they want greater control and choice over the disclosure of their private and confidential information. For instance, on April 6, 2000, our state's largest newspaper, the *Minneapolis Star Tribune*, published the results of a poll of more than 1,000 adults in Minnesota on telemarketing, telecommunications and internet privacy issues. A full 87% supported legislation banning commercial sharing of their telephone-calling and web-browsing habits without their permission. Indeed, just two days ago the federal banking regulators announced that they received **several thousand** comments from individuals in response to the Gramm-Leach-Bliley legislation, **"virtually all"** of whom encouraged the agencies to provide greater protection of individuals' financial privacy.

Consumer outrage over the unregulated, non-consensual trading of highly sensitive information will only continue to mount if Congress "studies" the issue. We do not need a multi-million dollar commission to study privacy for the next year and a half. The issues you propose to study are amply ripe for congressional action. I urge Congress to heed the call of the public and enact tough privacy legislation.

Thank you again for the opportunity to present my views to the subcommittee.

Sincerely,

MIKE HATCH
Attorney General, State of Minnesota

Enclosures

ATTACHMENTS* TO PREPARED TESTIMONY
FOR MINNESOTA ATTORNEY GENERAL MIKE HATCH
ON H.R. 4049

(MAY 12, 2000)

* Attachments are exhibits from the State of Minnesota vs. MemberWorks, 2nd Amended Complaint

SIGURD ANDERSON TRANSCRIPT

T. With your permission, I would like to tape record the confirmation of your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, okay? Now, I show the spelling of your last name as A-N-D-E-R-S-O-N.

C. That's right.

T. Your first name is S-I-G-U-R-D?

C. Yes.

T. And middle initial's A. I have your address as Rural Route 1, Box 171A. That's Lake City, Minnesota?

C. Yes.

T. 55041. Is that correct, sir?

C. That's correct.

T. Okay. Now, again, and again, Mr. Anderson, your membership materials will arrive shortly. After 30 days, unless we hear from you, the low introductory annual fee of $59.95, which works out to less than $5.00 per month, would be automatically billed to your [credit card name redacted] card account. For annual renewals we'll bill your account at the then annual fee. However, if you decide not to continue you just give our toll-free number a call. And finally, Mr. Anderson, just a quick survey question. Which one of these benefits sounds the best to you? Discounts on your music CDs and cassettes, discounts on videos, discounts on movie tickets, discounts on name brand items for your home? If you have no preference, I'll just put down that you . . .

C. It doesn't appeal too much anyway.

T. Yeah. What I'll do is just say that you had no preference and when you get your materials, just look over all of it and see which one you can use and best benefit from and, again, my name is Patricia Hunley and I'd like to thank you for uh - for trying Connections and if you have any questions, call one of our Connections service representatives and that number is 1-800, let me see what that number is. Hold on, I've got that number right here. Okay, it's 1-800-568-2386. And this number is also included in your membership kit. And you have a very nice day. Thank you. Goodbye.

AG: 370067,v.01

EXHIBIT
5

JOSEPH R. GWIN TRANSCRIPT

T. . . . your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, okay? Okay?

C. What?

T. Okay, sir, now with your permis- premission I would like to tape record the confirmation of your trial membership and your mailing address so there is no chance of any clerical mistakes on my part, okay?

C. Yup.

T. Okay. Sir, I show the spelling of your last name as Gwin, that's G-W-I-N, first name is Joseph. That's J-O-S-E-P-H. Is that correct?

C. (inaudible)

T. Okay, sir. And I have your address as 3455 173rd Lane Northwest. And that's in Andover, Minnesota 55304. Is that correct?

C. Yes.

T. Okay, sir. And again, Mr. Gwin, your membership materials will arrive shortly and after 30 days, unless we hear from you, the low introductory annual fee of $59.95 which works out to less than $5.00 per month would be automatically billed to your [credit card name redacted] card account. For annual renewals we'll bill your account at the then current annual fee. However, sir, if you decide not to continue just give our toll-free number a call. Now finally, Mr. Gwin, just a quick survey question. Which one of these benefits sounds the best to you? A discount on music CDs and cassettes, a discount on videos, a discount on movie tickets, or a discount on name brand items for the home? Or if you just like all the benefits. Do you have a preference, sir?

C. Not really.

T. Okay. Well, we'll note that. Sir, I really think you'll get a lot of use from your Connections membership. And sir, to help you get started when you receive your membership kit just go ahead and look through all of it to see how you can use all these great benefits. And again, sir, my name is Chris Sharborough. I'd like to thank you for trying Connections. And if you have any questions, sir, please give one of our Connections service reps a call at 1-800-568-2386. And sir, this number is also included in your membership kit. I thank you so much again, Mr. Gwin, and you have a great day. Thank you, sir, goodbye.

EXHIBIT
6

02/12/00 11:08 FAX 651 296 9663 MN ATTY GENERAL

Mr. HORN. We now have Mr. Robert Stone, who is the executive vice president of American Healthways. If you would, I would like you to explain what American Healthways is. I find it a rather unique operation.

STATEMENT OF ROBERT STONE, EXECUTIVE VICE PRESIDENT, AMERICAN HEALTHWAYS

Mr. STONE. Thank you, Mr. Chairman and members of the committee. Thank you for the opportunity to appear before you today.

My name is Robert Stone, and I am executive vice president of American Healthways, the Nation's largest disease management organization. I am also a board member of the Disease Management Association of America.

Today, American Healthways serves approximately 170,000 people afflicted with diabetes, cardiac, and/or respiratory disease and the more than 30,000 physicians who care for them. My oral testimony today highlights the written testimony already submitted to you.

How to protect individual privacy, particularly the privacy of personal health information, is extremely important. It is for this reason that we strongly support H.R. 4049. But in health care, perhaps more than any other area, balance is required. The proposed commission should therefore carefully weigh the protection of Americans from inappropriate uses of our personal information against the need to ensure access to that information for the effective provision of health care, particularly to the 50 million Americans with chronic disease.

No one understands the need for this balance better than patients themselves. With her permission, of course, let me share my wife's perspective. Having had Type 1 diabetes for 24 years, she frequently serves as my resident consumer expert. I asked her recently if her privacy would be violated if she received a letter from her health plan advising her of a program to help her better manage her diabetes; her response, a simple, "Of course not." Without further prompting, however, she went on to say she would be outraged if she then received a letter from a pharmaceutical company, a medical device manufacturer, or other organization trying to sell her a product or service related to her diabetes.

She recognizes, as do most consumers, that the motives behind the use of her personal health information in these two examples are clearly different. One is designed to help her, the other to sell her something by capitalizing on her illness.

It is disease management programs that provide the coordination, integration, and management of care processes necessary to help people with chronic diseases more effectively control their illness; and by improving overall health status, these programs also reduce health care costs. This is not wishful thinking. An independent analysis of our diabetes program confirmed that costs with 7,000 commercial HMO members in seven different health plans were reduced 12.3 percent in the first year.

Even better outcomes have been achieved and will be released shortly for more than 20,000 individuals participating in our program in four Medicare+Choice plans. Disease management programs depend on the free flow of patient information to provide the

customized proactive interventions which make these results possible. First, however, this information is needed to identify and engage program participants. After all, if we can't find them, we can't help them.

Our experience has shown if we depend on patient or physician referral as the entry mechanism, program participation levels are significantly lower—never greater than 30 percent, as compared to nearly 98 percent with a proactive engagement model—and the individuals who do elect to participate are the wrong ones, generally those who are relatively healthy, well motivated or who have good self-management skills. The people who both need and could benefit the most, nearly two-thirds of the total, are left out and the clinical and financial benefits are lost.

Is using personal health information to improve health status appropriate? Our plan customers, their members and the physicians in their networks must think so, since we have never had a single complaint in that regard. We have achieved that record through the use of stringent policies and procedures to ensure both confidentiality and security. The information to which we have access is never sold or disclosed to a third party, nor do we use our communications with participants or providers to advertise or market any drug, product or service.

Unfortunately, there are companies that do, and those inappropriate disclosures should be prohibited. Providing guidelines to distinguish between legitimate uses of personal health information and significant abuses of confidentiality is a worthy role for the proposed commission.

We would also ask that the commission be charged to issue a clear recommendation with respect to preemption. Currently, many State privacy laws directly conflict with each other, making it impossible for national employers in health plans, such as a Federal Express or a Cigna, to provide consistent programs to residents of different States. And as you know, the privacy regulations proposed by the Department of Health and Human Services, if and when issued, will not preempt State privacy laws. Only Congress can authorize preemption, and we urge that the creation of a single national standard be part of any further Federal legislation.

Ultimately, whatever legislation emerges from Congress must not inadvertently bar the use of personal health information to support better quality care and lower health care costs. The proposed privacy commission can help ensure this outcome by providing a clear road map through the complex privacy maze and distinguishing between appropriate uses of personal health information like disease management and those uses that are purely commercial.

Thank you for your time. I am pleased to answer any questions you may have.

[The prepared statement of Mr. Stone follows:]

3841 Green Hills Village Drive
Nashville, Tennessee 37215
Phone: 615.665.1122
Facsimile: 615.665.7697
www.americanhealthways.com

Testimony
of American Healthways, Inc.
before the
Government Management, Information and Technology Subcommittee
of the House Committee on Government Reform
regarding H.R. 4049,
the Privacy Commission Act

May 15, 2000

Mr. Chairman, members of the subcommittee, thank you for the opportunity to appear before you today. My name is Robert Stone and I am Executive Vice President of American Healthways, Inc. – the nation's largest disease management organization. Currently, we serve approximately 170,000 people afflicted with diabetes, cardiac and/ or respiratory disease, and provide support services to the more than 30,000 physicians who care for them. In addition to my role at American Healthways, I also serve as a charter board member of the Disease Management Association of America ("DMAA"). Both of these organizations have been actively involved in the privacy debate, having submitted comments on the record to the Senate Health, Education, Labor and Pensions Committee, the House Ways and Means Health Subcommittee, and to the Department of Health and Human Services with respect to their recently proposed privacy regulations.

Protecting individual privacy, particularly the privacy of personal health information, is extremely important. Because of the complex nature of this issue, however, even Congress has been unable to reach consensus and enact legislation. For that reason we strongly support H.R. 4049, Representative Hutchinson's bill to establish a Privacy Commission. This commission could thoroughly evaluate privacy proposals and provide recommendations to Congress for legislation that would ensure

both appropriate privacy protection and the absence of unintended consequences. In that regard, the charge to the commission should require that it appropriately balance the desire to protect all Americans from inappropriate use of our individual information with the need to assure open access to the information necessary to provide quality health care services to all, particularly to the more than 50 million Americans with chronic diseases.

No one understands the need for this balance better than patients themselves. Let me share, with her permission of course, the perspective of my wife who, having Type 1 diabetes for 24 years, serves as my resident consumer expert. When the privacy debate began to heat up last year, I asked her if she would feel her privacy had been violated if she received a letter from her health plan advising her of a new program designed to help her better manager her disease. Her response was simple, "of course not." Without further prompting, however, she went on to say she would be thoroughly outraged if she then received a letter from a pharmaceutical company, medical device manufacturer, or other company trying to sell a product or service related to diabetes. She clearly recognizes, as do most consumers, that the motives behind the use of her personal health information in these two examples are clearly different. One is designed to help her, while the other is trying to sell her something by capitalizing on her condition. One of the roles of the proposed Privacy Commission should be to distinguish between these different uses of personal health information.

The creation of a Privacy Commission to study the ways in which different industries, including the health care industry, do and should be allowed to use personal information will ensure proper protection for necessary and important uses. We know that privacy legislation is too important to be entered into lightly. The recent privacy legislation enacted, and ultimately repealed, in Maine provides a perfect, albeit extreme, example of the unintended but very real impact privacy legislation can have on patients and families. Maine's privacy statute called for complete confidentiality of patient information. Its impact hit hospital patients and their families in totally unintended and unexpected ways. Florists couldn't deliver flowers and clergy couldn't provide comfort

to patients because they were unable to determine if the patient was even in the hospital.

The Maine example points to some very obvious uses of personal health information that should be allowed. There are other appropriate uses of personal health information, however, that are less obvious and have a more significant impact on individual health and societal well being than a missed floral delivery. One of these is the provision of disease management services. To illustrate, I'd like to share with you how our disease management programs use personal health information in order to positively impact the care of some of the nation's most chronically ill individuals.

Disease management is a treatment support concept predicated on the simple principle that healthier people cost less. True disease management programs do more than just ensure that nationally recognized standards of care, such as getting annual eye exams for a person with diabetes or checking daily weights for a person with congestive heart failure, are met. Disease management is a multidisciplinary, systematic approach to health care delivery that:

- Supports the physician-patient relationship and plan of care,
- Optimizes patient care through prevention, proactive, evidence-based interventions and patient self-management, and
- Continuously evaluates health status and measures outcomes with the goal of improving health, thereby enhancing quality of life and lowering the cost of care.

Patients typically access these programs through their health insurer. Programs are either provided by the insurer itself or more often through contracts with disease management organizations like American Healthways. As a disease management provider, our goal is to help physicians, patients and health plans address the unique and complex health care needs of people with chronic diseases for the purposes of improving health status and consequently reducing costs.

The impact of our program is documented in clinical journals and increasingly in the press. For example, an independent, peer reviewed, seven health plan study of

7,000 people with diabetes found that our diabetes program significantly improved health outcomes. Hospital utilization decreased dramatically and there was a greater adherence to nationally recognized standards of care. As a result of these improvements, the program reduced health care costs by 12.3 percent or an average savings of $600,000 per 1,000 members with diabetes in the first year of operation. If you extrapolate this figure nationally, this program has the potential to trim $9.5 billion off the total direct cost of diabetes care in this country.

Outcomes from our cardiac program show similar results. For example, ACE inhibitor, cholesterol testing, and beta blocker compliance, the benchmark cardiac care outcomes measures, improved 23 percent, 61 percent, and 62 percent respectively, during the first year of program implementation. Costs were reduced an average of 62 percent for patients suffering from congestive heart failure.

And more good news is on the horizon. We will be releasing new findings in the next few weeks highlighting similar outcomes from our programs provided to more than 20,000 individuals participating in Medicare+Choice managed care plans. These findings, we believe, will have significant clinical and financial implications for the 10 to 18 percent of the Medicare population with diabetes including those in the Medicare fee-for-service program.

These successes stem from our ability to provide more services to people with chronic diseases, not fewer, and from helping to make people healthier and consequently less costly. But, our program, and others like ours, is dependent on open access to patient information. Accordingly, access to this information must not be inadvertently barred if patients, physicians, health plans, and society as a whole are to continue to derive these types of benefits.

Why is access to personal health information a critical success factor for disease management programs? First, identifiable health information provided by health plan customers is used to identify people diagnosed with the specific disease. Remember, if

we can't identify the patients, we can't help them or their physicians. Effective disease management programs will then automatically "engage" these individuals in the program, providing them with an option of leaving the program at any time. The initial information they receive about the program typically is provided by the plan, under the signature of its medical director. Each participant's physician is contacted as well. Good disease management programs don't leave physicians out of the equation because they are, after all, the true disease managers.

Many people argue that if disease management programs are so good, people with devastating chronic diseases would seek out these programs on their own. Health plans and disease management organizations then would have no need to access an individual's health information without consent. But experience has shown this not to be the case. For example, programs that rely on individuals to take the first step see participation rates of less than 30 percent. Moreover, it is the wrong 30 percent opting to participate. This percentage typically represents well-motivated individuals who have strong care management skills. As a result, the higher risk individuals who need the most disease management assistance don't benefit from what the program has to offer. In contrast, programs that use personal health information to identify patients and actively reach out to them achieve more than a 97 percent participation rate. This dramatically higher participation rate means that more than three times as many people are benefiting from additional services and early interventions.

Second, once individuals are part of the program their health information is used for a variety of purposes including:

- Customizing interventions and care plans to meet each participants individual needs depending on the severity of their disease,
- Coordinating both preventative and immediate health care needs across the entire delivery spectrum, and
- Designing targeted educational programs.

This information also helps physicians and participants benchmark their success, identify possible problems early and then modify treatment programs. Ultimately, the result is a stronger patient-physician relationship, a healthier population, and lower overall health care costs.

Is this an appropriate use of personal health information? Our health plan customers, the physicians in their networks, and our 170,000 program participants think it is. Our customers clearly recognize that for their members with chronic diseases, their expertise lies in handling administrative functions and utilization management, and not in the comprehensive coordination, integration and management of care. This is why they turn to us for help. Our program participants are highly satisfied as well. Our most recent satisfaction survey found that between 93 and 97 percent of participants are satisfied with the way the program provides information, applies to their lifestyle, and helps them stay well. They regularly praise our staff for helping them navigate the increasingly complex health care system to get the services they need to stay healthy, happy, and productive in their day-to-day lives.

Physicians feel the same. Recent surveys show that nearly 90 percent are satisfied with the importance the program plays in improving their patients' overall health, and more than 80 percent are satisfied with the way the program performs.

One reason that our participants and their physicians feel this way is that we have stringent policies and procedures in place to ensure the privacy of their health information. In fact, in the 15 years we've been working with people with chronic diseases, we've never had a single complaint regarding breach of confidentiality. The information to which we have access is never sold or disclosed to a third party. Nor do we use our communications with participants or providers to advertise or market any drug, product, or service. Unfortunately, there are companies that do. These organizations have clearly conflicting interests and should be prohibited from either having access to patient identifiable information or from using it for non-care related commercial purposes.

The most important thing to remember, however, is that the fundamental transaction in health care is the one between the patient and his or her physician. Everyone else involved in the health care industry is there to support that relationship and to help to make it more effective, more efficient, or both. Health care organizations, including disease management programs that have any other purpose are at odds with this underlying principle.

Clearly there are circumstances in which access to personal health information can benefit the patient and society. The proposed Privacy Commission would provide an excellent forum to examine all current uses of personal information, in order to identify those legitimate uses as well as to protect against abuses.

In addition to assessing appropriate and inappropriate uses of personal information, the Privacy Commission also should assess how privacy proposals at the state and federal level are linked. For example, regulations proposed by the Department of Health and Human Services include disease management under the definition of "treatment" and, therefore, use and disclosure of identifiable health information for disease management is permissible without individual authorization.

The HHS regulations, however, do not and cannot preempt state privacy laws. Complete federal preemption is imperative. Maneuvering around the varying and often incompatible requirements of so many state laws is difficult and will become more so as more states begin to pass their own legislation. Some state privacy laws directly conflict with others, making it impossible to provide the same, consistent services to residents of different states. Health plans that contract with national employers (e.g., Federal Express) want and need to provide a uniform set of benefits to all their employees. This is impossible with the varying and often conflicting state laws and requirements. In addition, a health plan that is national in scope (e.g., Cigna) needs the ability to sell and deliver uniform products, again extremely onerous, if not impossible, without one uniform standard.

Ultimately, whatever privacy legislation emerges from Congress must weigh the privacy of individual health information over the real need to improve the health status of Americans and reduce the costs of delivering this care. The Privacy Commission proposed in this legislation can help ensure that this need is not overlooked while at the same time provide you and your colleagues with a clear roadmap through the privacy maze. The worst possible outcome is that without that roadmap you and your colleagues might not pass privacy legislation at all.

I am happy to answer any questions you may have and I thank you for your time.

Mr. HORN. Thank you. That is very helpful and a different type of statement.

We will now go to questions and answers. The Members here, we are going to limit each to 5 minutes, and we will rotate until you are all worn out, so it will keep it interesting with three of us here.

I will start with the first gentleman, who is the author of the legislation, Mr. Asa Hutchinson of Arkansas, for 5 minutes on questioning the witnesses.

Mr. HUTCHINSON. Thank you, Mr. Chairman. I want to recognize Mr. Moran who came into the room, my cosponsor on this, and thank him for his active participation and support for it. I do thank each of the witnesses for their excellent testimony and presentation and differing viewpoints on this subject.

Mr. Spotila, let me start with you, expressing the administration's viewpoint, and thank you for emphasizing the common ground that we have sought.

You mentioned the administration's work in this regard and that you don't want a commission just to duplicate what already is out there. You cited a number of different commissions. Let's see here—which is really the interagency privacy working group, and the ones that you have cited here are agency driven; am I correct?

Mr. SPOTILA. They are either agencies themselves or interagency groups.

Mr. HUTCHINSON. Which is very important. I make a distinction between a congressionally mandated approach to privacy versus an agency.

Mr. SPOTILA. We do defer to a considerable degree to the Congress in whatever you believe is appropriate to help inform your judgment. Our concern is not delaying doing things that are needed now.

Mr. HUTCHINSON. Your point is very well taken, and I would emphasize the same point that you just made, that the intent of this legislation is not to infringe upon the agencies as they move forward. In fact, it is not going to stop. You've got them moving forward into a final rulemaking position here long before the commission will render any results.

Mr. SPOTILA. Clearly, we would continue to move forward in areas where we could. There are legislative proposals in front of the Congress that we think are urgently needed and so we do have some concern, if the Congress were to halt its action pending the report of a commission.

We also were attempting to share some of our experience, and that is where we have found the greatest success has been in very focused, targeted efforts rather than broad ones. This is a huge topic. It is easy to be a mile wide and an inch deep. That is not very helpful.

Mr. HUTCHINSON. I think part of your point is well taken. Let me just respond in a couple of ways.

First, I think the work of the agencies is very important. They have a lot of expertise in narrowly starting targeted areas. So I think that is important. Again, I view this commission as complementary to that.

Even if all of these regulations move forward without any controversy, would you agree with me, 3 years from now we are going

to need to continue to review, whether through the agency or the legislative body, the issues of privacy?

Mr. SPOTILA. Absolutely.

Mr. HUTCHINSON. Again, you make the case just by that answer that it is an ongoing effort on privacy and there are things—I have cosponsored legislation that ought to be done now. But if everything on the table is adopted, we still need to have a comprehensive review of it, as well, would be my case.

When was the last time, to your knowledge, there was a legislative effort/commission that reviewed privacy?

Mr. SPOTILA. I don't recall one certainly in recent times. We can try to be more specific, but personally I don't recall one recently.

Mr. HUTCHINSON. I would agree with you not in recent times. I wouldn't consider 1974 recent, particularly in view of the technological developments. I saw the 1974 legislative commission report, and it was talking about privacy in the Information Age. Well, the Information Age has dramatically changed since 1974. So there has been a lot of agency work, but not legislative work.

You make the point that if the commission is adopted, that it should not be just going on and on without having anything accomplished in the short term. You mention that it should be done within a short timeframe.

Do you believe that an 18-month commission is too long or too short?

Mr. SPOTILA. I think that our concern is that the combination of a broad list of topics and an 18-month timeframe suggests that the commission will not be as helpful as you might like it to be; that targeted efforts that zero in on particular aspects of privacy with a shorter timeframe, that inform decisionmakers in concrete terms, will prove more useful.

Mr. HUTCHINSON. I want to invite you because your point as a concern has been expressed by others. The broadness—there is some benefit because you are able to look at—rather than a sectorial approach, you can look at it in a comprehensive standpoint all across the line from on-line privacy, which transects everything from medical records to educational records, so there is some merit to that.

Also there is the danger of the commission having too much to do and they don't know where to start.

I would welcome your view as to ways that the commission can be pointed in the right direction; we would solicit your views on that. I would point out that the 18-months is the deadline, the drop-dead point. It is not just an ongoing thing, it is going to cease to exist after 18 months. And it also provides, if the commission deems it appropriate, they could issue a report before then if there are some urgent matters to address.

Do you believe that it is appropriate that you have an 18-month deadline, that you can't go on beyond that?

Mr. HORN. We will have further rounds, but let's respond to that question, and then we move to Mr. Moran.

Mr. SPOTILA. I think it is important to have some outside date, clearly. I think our instinct is that 18 months may be too long, but this is also related to the nature of the topics that it would be look-

ing at. We would be happy to continue to work with the committee and with the Congress to try to refine these approaches.

Mr. HUTCHINSON. Thank you.

I want to assure the other gentlemen that I have additional questions. I was just taking them one at a time.

Thank you, Mr. Chairman.

Mr. HORN. I am now delighted to yield 6 minutes to the gentleman from Virginia, Mr. Moran. If you have an opening statement and you want to read some of it in, we will give you additional time.

Mr. MORAN. Well, thank you very much, Mr. Chairman. I will just make some introductory comments. The first comment, of course, is to thank you for having these hearings and to thank my cosponsor, Mr. Hutchinson, for his excellent leadership on this issue.

We know that the loss of personal privacy is a cutting-edge issue and one of the topic issues that confront Americans today. Personal medical information that is kept, stored, transmitted, distributed to people without an individual's knowledge makes them vulnerable. We know that profiling has taken place among a number of electronic commerce companies, presumably for the benefit of their customers, but obviously for the benefit of companies and oftentimes without the customer's knowledge.

But we also have to recognize that the reason—one of the reasons at least that the United States is the leading economic and social force in our global economy is because we have such a favorable regulatory environment, so new ideas, new ventures can sprout up, take form, and become successful.

We don't want more regulation than is absolutely necessary, and I think the history of our economy has proven that that should be the way in which we ought to operate. But the U.S. Internet economy is now worth over $350 billion. I think we have about 72 million American adults using the Internet today, and those numbers are increasing; and as they increase, obviously privacy is going to continue to be an acute concern on the part of the people who use the Internet.

So our conclusion, the reason why we came up with the bill is that we need a thoughtful, deliberative approach to a very complex subject. And that is what we try to do. Maybe we have too many members, but every group that I have talked to wants to be represented so that is why we have as many as 17 members. And if it is as difficult an issue to come to grips with and to come up with constructive recommendations, we want to give an adequate amount of time; and that is why we came up with about 18 months.

I know Mr. Hutchinson and Chairman Horn have had this experience, any number of companies coming to us and showing the technology that is developing, as we speak, that enables the industry to self-police itself, to self-regulate itself, but we still don't know what the proper role for the government is and it would seem that there is a critical role for the government to perform.

So that is the environment in which we have this hearing.

First of all, Mr. Chairman, I want to ask that two of the speakers who wanted to present their testimony, Willis Ware, he used to

work with the RAND Corp., he has some very interesting testimony; and Marjory Blumenthal, who is the Director of the Computer Science and Telecommunications Board for The National Academies, both speakers wanted their statements included for the record so we ought to do that.

[The prepared statement of Ms. Blumenthal follows:]

For the record

Written Statement

of

Marjory S. Blumenthal
Director
Computer Science and Telecommunications Board
Commission on Physical Sciences, Mathematics, and Applications
The National Academies

on

The Proposed Commission for the Comprehensive Study of Privacy Protection

Submitted to the
Committee on Government Reform
U.S. House of Representatives

May 15, 2000

Marjory S. Blumenthal
Written Statement
Page one

This statement is intended to provide input into the consideration of the proposed Commission for the Comprehensive Study of Privacy Protection, addressed in H.R. 4049. It draws from my experience as the director of the Computer Science and Telecommunications Board (CSTB) of the National Academies, as well as prior experience in the former U.S. Congress Office of Technology Assessment. The National Academy of Sciences was formed in 1863 by congressional charter to advise the federal government. CSTB, which dates to 1986, is chartered within the National Academies to address the full range of technical and policy issues associated with information technology (see www.cstb.org), and it has conducted several major, influential studies relating to privacy and security (security providing context in terms of vulnerabilities, threats, and attacks on privacy and mechanisms for preventing, detecting, or recovering from same).

The need for thorough consideration of U.S. privacy policy and the risks and opportunities to privacy presented by information technology is self-evident—incidents relating to privacy on the Internet are the stuff of daily news, as well as congressional hearings and federal agency inquiries. At issue is the scope of what would be useful and how to proceed. This statement comments briefly on each.

The scope of study proposed appropriately includes both government (at multiple levels) and private sector activities, which each raise privacy issues separately and in their interrelation. Beyond that, the written description in H.R. 4049 is at such a high level that the coverage of various issues is hard to ascertain (e.g., attention to employer-employee rights and responsibilities, effectiveness as well as potential for self-regulation v. government regulation, evolving technical capabilities that promote or contain privacy risks, procedural options that promote or contain privacy risks and their relation to technical mechanisms, expectations for changes in circumstances over time and the achievement of flexible approaches that are responsive to such changes, and so on). The proposed report contents, for example, call for comment on the "purposes for which sharing of information is appropriate and beneficial to consumers," but the hard problems relate, as they often do, to the details: how much of what kind of information would achieve what benefits, to whom, and at what costs, to whom? What are the choices and tradeoffs?

The complexity of the situation should not be underestimated: as CSTB illustrated in its assessment of the privacy of electronic medical records, *For the Record* (National Academy Press, 1997), the electronic capture and communication of sensitive personal information is expanding from multiple sources, while the set of parties with some interest in or expectation for access to that information is also expanding, and there are

numerous choices that can be made by different classes of individuals, organizations, industries, and government entities at various levels, only some of which may be captured by institutional and/or government policies. CSTB's assessments of cryptography policy and of government systems modernization projects make clear that balancing high-level public and private sector interests can be difficult, let alone conflicting interests within the private sector (or within the public sector, for that matter). Further, the global nature of the economy and increasing numbers of information flows makes it important to view U.S. circumstances from an international perspective, as recent negotiations with the European Union have made clear. Therefore, the remainder of this statement will concentrate on questions relating to how to proceed in studying privacy issues.

A critical element of a study is the selection of the participants. H.R. 4049 focuses on political distribution of participants and their selection without comment on their intellectual and attitudinal qualities. CSTB (and the National Academies generally) use processes aimed at developing study committees with diversity of many kinds, providing a microcosm of the differing relevant perspectives. Elements of these processes, which are labor-intensive, include the following:

- Staff casts a wide net, through conversations with known experts or proponents of differing views and written and oral solicitations of nominations from a wide range of organizations (scholarly, business, professional, nonprofit) and individuals (knowledgeable authorities on the topic), to generate a list of candidates for the committee.

- Committee candidates are organized to provide sets of alternative choices for categories of committee membership that are differentiated by kind of expertise and outlook on the topic. Primary experts are sought, as opposed to designated policy officials of, for example, trade associations. Individuals are nominated as individuals, on the merits of their expertise and potential to contribute to the committee, not as representatives of specific organizations.

- Selection of the sets of candidates by category factors in additional kinds of diversity, including geographic, demographic (sex, race/ethnicity, age), and affiliation (e.g., different kinds of industry, university and other scholarly institution). Affiliation, like public statements and other expressions of opinions on the topic, are characterized as the "biases" of committee members, and effort is made to balance biases, that is, achieve a range of outlook and opinion that will promote balanced consideration of the issues. By contrast, people who are believed to have a conflict of interest, defined as an ability to profit directly, personally, and significantly from the plausible outcome of a study, are excluded from membership.

- The full set of nominated candidates is reviewed at multiple levels within the National Academies and ultimately approved by the president of the National Academy of Sciences, with the review considering the balance and composition of the proposed committee as well as the caliber of specific nominations. Following acceptance of an invitation to serve, the names, affiliations, and brief biographies of the proposed committee are posted on the National Academies Web site for a period of public comment before committee membership is deemed established.

Selection of a committee chairperson involves the same processes, but often occurs early on, so that that individual can assist in the composition of the committee. It is important that the chairperson be perceived as without bias on the topic and broad in outlook and/or knowledge, as well as demonstrably capable of listening and leading.

Another critical element is the nature of the outcome. At the National Academies, we often strive for a consensus report. With a contentious, charged topic, that can be difficult, but even a consensus description of the problem and framing of options can help to advance the debate. It may be inevitable with a congressional commission, as suggested by the recent commission experience relating to taxation of commerce over the Internet, that the political nature of the process hampers achievement of consensus; the language calling for a majority report and inviting dissenting minority report reinforces the likelihood of a failure to achieve consensus and sends a signal that consensus isn't important. If that is true, however, it calls into question the value of a commission as compared to one or more hearings that feature differing points of view, and it also raises questions about how to tailor the scope of inquiry to fit the means. That is, if the means are likely to be politicized, should the scope be narrower to increase the likelihood of a useful outcome?

Consensus in this arena will be difficult. At CSTB we have seen that even in such areas a cryptography policy (*Cryptography's Role in Securing the Information Society*, National Academy Press, 1996) and intellectual property in the Internet environment (*The Digital Dilemma*, National Academy Press, 2000), it is possible to achieve consensus from a mixed, representative group on important points. Doing so is not easy; it takes time for people to be exposed to a wide range of inputs and perspectives, to argue and deliberate, and to work out differences and careful wording. The National Academies process provides a neutral, apolitical meeting ground and experienced professional staff support that foster inquiry, discussion, and agreement. The emphasis on committee deliberation contrasts to the approach of the former Office of Technology Assessment and many think-tanks, which consult with outside experts but rely on staff to formulate the analysis and conclusions. That process is perhaps more efficient to execute, but it is one step removed from the more direct expression of a mixed group.

A comprehensive examination of the technical, economic, social, and legal dimensions of the privacy policy challenge would be valuable. It is high on the list of CSTB's own objectives, because of the compelling need and the value of a neutral, balanced analysis at this time. I am pleased to contribute to the Committee's evaluation of a proposed approach to the problem, and I forward to the outcome of this process and to contributing further to progress in this important area of public policy.

Mr. HORN. Without objection, those statements will be put in the record. At the end of the hearing you might want to read some pertinent paragraphs.

Mr. MORAN. Thank you, Mr. Chairman. I wanted to make sure that I didn't forget, and I know that you keep the record open for a couple of weeks.

[The prepared statement of Hon. James P. Moran follows:]

STATEMENT OF
CONGRESSMAN JAMES P. MORAN. JR.
BEFORE THE SUBCOMMITTEE
ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
HEARING ON HUTCHINSON/MORAN PRIVACY COMMISSION ACT

May 15, 2000

CHAIRMAN HORN, MEMBERS OF THE SUBCOMMITTEE, Thank you for the opportunity to appear before you with Congressman Hutchinson for this hearing on H.R. 4049, the Privacy Commission Act.

Americans are more and more aware and concerned that their personal information is not as secure as they would like. In fact, in a Wall Street Journal/NBC News poll last fall, loss of personal privacy ranked in the top list of issues that concern Americans in the new century.

These 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. 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, there are no uniform standards ensuring individuals' protections.

At the same time we must recognize that the United States is the leading economic and social force in the global economy, largely because of a favorable regulatory climate and the free flow of information and there is a danger of over-reaction in privacy regulation.

The U.S. Internet economy is already worth an estimated $350 billion. 72 million American adults, some 35 percent of the American population, are expected to be on-line by the end of this year. 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 that what is needed is a thoughtful, deliberate approach to privacy issues by Congress.

This 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 in Congress to examine the threats to the privacy of Americans and to report back on what legislation may be necessary.

It also directs the Commission to report on non-legislative solutions. If self-regulation can be improved, how should industry achieve it? 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.

In short, this is a balanced, measured approach to a complex issue. I commend Mr. Hutchinson for his leadership on it and I commend this committee for holding hearings on this subject.

Mr. MORAN. Now, the question that I was most interested in asking was, first of all, Mr. Spotila, who is—you represent the administration on the panel. We have had some prior efforts to come up with studies relevant to consumer privacy. I know with regard to medical privacy issues, HHS took up a major privacy regulation—effort, last year.

Now, recommendations were made in September 1997, and a proposed rule was made in November 1999. I understand that HHS's efforts to examine medical privacy included a number of consultations with various Federal agencies, and any number of hearings as well; and the comments that they got were in the tens of thousands.

Do you have any idea of the time and resources that were required by the Department of Health and Human Services when—in their preparation for coming up with the regulations that were required in 1997, and which were finally issued last year? Do we have any idea of the cost that was encompassed by performing that task?

Mr. SPOTILA. I don't have, offhand, a dollar aggregate cost. Clearly, there was a period of time when the agency was waiting to see if Congress would take action; and then certainly last year there was a major effort in which my office participated in working with the Department to prepare that proposed rule.

There was a team working at HHS on this subject. They worked intensively on drafting the provision. The proposal did get something like 53,000 comments. You are correct, we received widespread public reaction to the proposal and, of course the Department is looking right now at trying to finalize that rule before the end of the year. If it is important, we certainly could inquire and provide for the committee whatever financial or economic estimates there might be from the Department as to what that aggregate cost would be.

Mr. MORAN. I think it would be an interesting consideration. And similarly, the legislation on financial services modernization required a similar type of study, and I think it would be useful to know the resources that are being required to conduct that study, as well, because both studies seem to be relevant to the subject at hand.

Mr. SPOTILA. We can reach out and attempt to get that information and submit it to the committee.

Mr. MORAN. Thank you, Mr. Spotila.

Mr. HORN. We will put that in the record at this point without objection. The 6 minutes plus I believe has expired. But we will get back to that.

Mr. MORAN. Thank you, Mr. Chairman.

Mr. HORN. Let me get my 5 minutes in.

Mr. Spotila, I am curious, what is your view of Mr. Stone's objection to the preemption of State law?

Mr. SPOTILA. In general, we are deferential to State law and to the desire of States to have stronger privacy protections. That has been the approach we have engaged in, and we are sensitive from a federalism standpoint to that type of approach. We realize that there is benefit from having a common standard, and Mr. Stone

was alluding to the difficulty that can occur if there is a hodgepodge of different standards that may not be consistent.

So I think there is a need for balance. Our approach has been to try to zero in on things that we felt did have common application and that could form a basis, but not necessarily to preempt altogether an area where the States have strong interest and where they have had a historic activity.

Mr. HORN. Well, there is no question that industry and other entities across America would like one policy and not 50 policies. But I do remember in this room a few years ago when we had the frozen chicken hearing and that was because Tyson and whoever else was running the Department of Agriculture, so they had a softer freezing thing and California had a very high standard.

I think it is still that way. California has a high standard, but they were preempted by the Federal Government with a weaker standard. So I wish you well when you are trying to get a higher standard, because I think that is what we ought to be moving for where we can, but we don't want to disrupt the whole economy in the process.

I will be getting in, with some panels, the European situation where every country in Europe is supposed to be putting a privacy law on the books, and that will be a real problem for American industry, and I have talked to a number of presidents, prime ministers, defense ministers, foreign affairs ministers and urged them to get subcommittee—or subcorporations of European corporations and American corporations to give them some advice on the practical aspects of this.

Has your office done any of this in relation to the Department of State?

Mr. SPOTILA. We have had some contact. Peter Swire has had some coordination contact with European Union issues. In fact, he is something of an expert from his work in the world of academia.

I would emphasize also that we strongly encourage self-regulatory efforts. We do so not only because that is always a good thing to do but because very often with well-intentioned and interested private sector parties, we can come up with better and more sensible approaches. So our sense is that any approach, Federal or State, should allow substantial room for private, self-regulatory efforts as well.

Mr. HORN. What evidence do you have that the commission could result in delays in the development of the privacy initiatives?

Mr. SPOTILA. It is a general concern. We have seen some suggestions that people who oppose privacy reform would welcome any effort to add delay. My colleague from Minnesota was mentioning this: now you have a commission, why don't we wait a year and a half and hold up everything until the commission has reported?

That is exactly what we think would be a mistake. I recognize that you emphasized that is not the intention here, but there is concern that there are those who might use it in that way. We have to be sensitive to that concern in considering any approach like this.

Mr. HORN. Well, I would think with 17 people there, there could be a majority. I think if it is broadly spread out among the various interests and not just one interest or two interests, I would think

that kind of dialog and discussion would be worthwhile. I think back to the Hoover Commission in the late 1940's and the early 1950's, and that made major proposals to the Federal Government and a lot of progress was made. And what I have found over the years, if you don't have a mechanism which brings people together, gets a consensus, that you are just going to be spinning the wheels in Congress, and you would be better off having a group of people, including experts and others, who just ask the question, "Why? It sounds dumb to me, now explain it to me. If you go through that process, you are more likely to get legislation out of the Congress, I would think. But you might take a look at it.

And then I guess I would ask you, Mr. Spotila, what section of the bill puts at risk the release of classified information? Where do you see that in the bill?

Mr. SPOTILA. This was a relatively late concern that we received from the National Security Agency and the Department of Defense. Their concern was that some of the broader references to the commission getting information from the agencies failed to make a distinction as to the handling of classified information. So our sense is, that is something that bears further discussion. I would be happy to get back to you more specifically with that, although I don't have their specific recommendation for how that might be addressed. They certainly do feel there ought to be some specific approach to classified materials to the extent that they might be drawn in.

Mr. HORN. Well, since Mr. Hutchinson is next with 5 minutes, you might want to continue that discussion, and I am sure he has many more questions. We would like to know where he thinks this great power is found.

Mr. HUTCHINSON. Thank you, Mr. Chairman.

I would very much like to address a concern which has been raised on national security issue. That seems relatively simple to fix, but very important and it sounds like you have put out a request to different agencies, maybe responding to the commission idea and getting some feedback; and I would love to have the benefit of any concern, positive or negative, about the commission.

Mr. Veator, thank you again for your testimony. If you would give my regards to Lieutenant Governor Swift, I enjoyed and appreciate her work on privacy. And one thing that struck me about your testimony is that you mentioned two or three bills are pending in State legislatures dealing with the privacy issue now. In your State of Massachusetts, have you all passed any substantive privacy legislation?

Mr. VEATOR. I think that there are—the short answer is no, I think not in the last year or so. There are several bills that are quite close, working their way through the legislature relating to—primarily to medical and health privacy. There are two bills relating to financial service, primarily to financial services privacy.

Mr. HUTCHINSON. Are you aware of some States that are using the commission approach to developing their own State policies on privacy?

Mr. VEATOR. I am not aware of other States, just our experience where we tried to pull together as many people we could with diverse stakes, if you will.

Mr. HUTCHINSON. General Hatch may be aware of that. Are you aware of any States, Mr. Hatch?

Mr. HATCH. In Minnesota, we did try to appoint a task force. The problem is it ends up being, as you have indicated, a lot of interest groups. The purpose of a task force is to do one of three things: either find out the technology of an issue that we cannot as lay people figure out; second is develop, by consensus, on an issue that we cannot get people to agree; and the third is to avoid the issue altogether.

In this case, there is no science. There is science creates the issue. The technology brings in part the issue, but it is not a hard one, a fundamental issue of privacy. It goes back to the beginning of this country and even further than that. It is a value issue. Restatement of torts, courts have covered it, statutes have covered it.

It is not a consensus. We will never get a consensus on it. You have got too many companies that make exchange on the data, too much legal and I think questionable activity that goes on by the use of the information versus the fundamental right of privacy. So the third becomes the issue to defer.

When we tried it, we quickly recognized that it doesn't work. You are not going to get a consensus on it. The first meeting we figured that out. It isn't going to occur.

Mr. HUTCHINSON. Mr. Hatch, if I might follow on on some of your comments, I think you are right. I think a task force, or in this case a commission, can do a number of things. One is to help build a consensus. You also mentioned the possibility of delay. And again that is not the intent, nor do I think it should be the result. I think it can be a very positive thing. But a consensus to me is important.

You have introduced legislation in your State of Minnesota addressing privacy, and I think specifically toughening up the opt-in on the financial records.

Mr. HATCH. Right.

Mr. HUTCHINSON. Has that passed?

Mr. HATCH. It's passed one house and hopefully we have 2 days left, we can get the other house to do it. But we have 59 hurdles to overcome to get to those votes.

Mr. HUTCHINSON. You have 59 hurdles in Minnesota. We have 435 hurdles in the U.S. Congress. And so consensus is important for us to build as well. And I disagree, I think that, you know, you indicate that the American public either believe or don't believe or industry believes or don't believe. I think information is crucial. And I think that one of the things this commission provides is that you have hearings. And it's not just to receive information, but it's also an education process. People have a great understanding as to how privacy can be protected, but also that some exchange of information in terms of health records or health might be important for research.

So information is valuable in building that consensus, and so I hope that that would be the goal of this commission.

Mr. Chairman, you were generous to offer to put things in the record. It was pointed out by your staff that the committee received a letter from the office of the Attorney General of the State of Texas, and has that been made a part of the record yet?

Mr. HORN. I was planning to make it at end of the hearing and quote various paragraphs.

Mr. HUTCHINSON. Well, this is your thunder, but I was going to ask whether Mr. Hatch—General Hatch, if other Attorney Generals that you have talked to have looked at privacy in their States in terms of whether it should be the State level multitude of layers of privacy or whether there should be a national standard. Has that been addressed?

Mr. HATCH. We've had discussions on it. I think it is safe to say that most, I won't say all, but many of the Attorney Generals are in agreement that it ought to be. It is a part of the police powers of a State and it ought to be addressed at the State level. It certainly ought to be addressed at the Federal level. I think the confidence level that Congress will address it is very low. We saw that with FSMA. The bill passed and it was basically dressed up as a basic privacy act, but it was a bank disclosure act. Banks have more authority to disclose information.

Mr. HUTCHINSON. Are you speaking of the Gramm-Leach-Bliley legislation that provided for an opt-out provision?

Mr. HATCH. Actually, it provided for, sir, a provision to trade information without an opt-out to any affiliate. It allows them to trade information without an opt-out to any other company for the sale of financial products, and then it defines a "financial product" very broadly. So it basically did little, if anything. There would be an argument that it tromped on the fiduciary laws that have been enacted and have been longstanding in many States.

Mr. HUTCHINSON. I think my time has expired, Mr. Chairman. I was going to have Mr. Spotila respond to that from the administration standpoint, but I yield back to the Chair.

Mr. HORN. Go ahead. We will give Mr. Moran extra minutes.

Mr. HUTCHINSON. Mr. Spotila, do you believe that we should have Congress address further the Gramm-Leach-Bliley provisions that the Attorney General just referred to?

Mr. SPOTILA. It is our position that the statute was a step in the right direction, but it did leave gaps that do need to be addressed.

Mr. HUTCHINSON. And right now the administration is adopting the regulations to carry that out. There is legislation pending that would adjust that. It is my judgment, there—this legislation might move forward. And if it can, terrific, if you can build a consensus. But would a commission, though, looking at this from a substantive standpoint, look at the impact of your regulations that the administration is putting out and how industry is adjusting to that, getting consumer feedback; the commission would take that and make a recommendation from there. Would that not be helpful in building consensus to move forward?

Mr. SPOTILA. Actually, this is an interesting point, because as I mentioned in my testimony, one of the areas we have a lot of concern is that the commission might be a reason for people not to take action on financial privacy legislation that we think is clearly needed after that statute. If that financial privacy legislation did move forward and the commission was now studying what, if anything else—assuming there was a commission—what, if anything else, was needed after that, without having delayed this process, the argument for it would I think be stronger than if it were to

suggest that we should hold up completely financial privacy legislation and let the commission try to develop consensus and look at this in a couple of years.

Our sense is that this is a more urgent priority and that part of the challenge here as the Congress considers this bill, is how it might form a mechanism or create a mechanism that would allow us to consider that longer view in studying these issues without paralyzing us in areas that are of real priority, where action is clearly needed and needed more swiftly.

This is actually one of the most sensitive areas about the bill and one that gives us some discomfort for this reason.

If I might add, as to your earlier question on the issue of classified information, the language in section 7(c), which indicates that the commission may secure directly from any department or agency information necessary to enable it to carry out the act, and that the head of that department shall furnish that information to the commission, is the language that the agencies specifically are concerned about because it does not differentiate whether that information is classified or not. And there is no provision here that indicates the commission is equipped to handle classified information.

So that is the specific provision that we are concerned about. As to how, if at all, that could be refined, we would have to get back to you.

Mr. HUTCHINSON. Thank you, Mr. Chairman.

Mr. HORN. The gentleman from Virginia. We are going to start 10-minute rounds now. It is like a dance out of the 1930's. So go ahead, my friend.

Mr. MORAN. Thank you, Mr. Horn. I don't want to put our witnesses through too long a marathon session. I will try to wrap up any further questions I have at least today in this round.

Let me ask Mr. Spotila again, in light of the efforts that were made with regard to medical privacy culminating in the regulations in August 1999, and the financial services modernization effort that is currently being made, has OMB done any preliminary analysis as to what resources might be required to perform the kind of commission that we are talking about? Has there been any discussion in that regard?

Mr. SPOTILA. I'm not aware of OMB having tried to estimate the cost of the commission. That's not necessarily something we would try to do. I'm sure if you would like us to, we could try——

Mr. MORAN. Have there been discussions at OMB as to the benefit of having a comprehensive study instead of the ad hoc reactive study as a result of legislation, whether it be in medical privacy or financial privacy areas?

Mr. SPOTILA. There has been discussion not only within OMB, but within the administration on this issue of what I call the more targeted approach. When it works well, it is targeted and focused and very pragmatic, it doesn't, it is very ad hoc and kind of irresponsible. This is versus a broad approach which might be either visionary or a waste of time. We have had a lot of discussion about this.

Our concern is, that if the commission is focused on too broad an area, than it won't produce much of value, and if its timeframe is too distant, it might not inform decisionmakers on matters that

need more urgent attention. That is not to say that it is impossible for a commission to add value. That is not what we are saying at all. We do have concerns about how this balance might be struck, however, and concerns that the way the bill is crafted now, it might not be striking the balance correctly.

Mr. MORAN. Give me a moment to consider what you just said, that you might not be striking the balance correctly. I would not have been surprised if the administration had recommended a broad study so that it could make its recommendations in a consistent framework, particularly given the resources that are currently going into the information security effort, which is very much related to this.

Mr. SPOTILA. Yes.

Mr. MORAN. And I know that those efforts are substantial. They are being coordinated—actually, we are trying to figure out the best place for it to be coordinated. But there is an office—you are involved in that coordination?

Mr. SPOTILA. Yes, I am.

Mr. MORAN. And it would seem that when you make broad-based policy recommendations that are applicable to medical privacy, that there should be some consistency in terms of individual privacy with regard to financial services as well, and that would include profiling issues, the issues of shared information that enhance customer service.

So I guess I was a little taken aback, or questioning at least, of the effort on the part of the administration to take a position that we need legislation immediately. And I'm referring to the President's recent speech that protected people's privacy without having a good idea of how it is that you want to do that beyond what was included in the medical effort that HHS conducted. In terms of financial services, we haven't done it yet. I mean, we've got legislation. Regulations haven't actually been issued. And my interest is in trying to keep the issue from being politicized and to put forward legislation that not only stands the test of time, but has some consistent principles that are applied broadly, whether it be in medicine or financial services or in any other area of electronic commerce and communication.

But I'm not lecturing you. I just wondered—do you have any comments on that before I go on?

Mr. SPOTILA. Again, when I talked about striking a balance, what I meant to say was that we see pressing needs in the area of protecting privacy, financial records, medical records, genetic discrimination. There are pending legislative proposals in front of the Congress that we believe are well conceived and well drafted. They could perhaps be refined further, but they are good pieces of legislation and we do not want to see those bills frozen because a commission is set up to look at the whole subject of privacy in all of its ramifications.

Now, having said that, that does not mean that we don't share your sense that privacy is important and that we need to study it in a comprehensive way and that we will need to be doing this over a period of time.

Mr. MORAN. And that we need some consistent principles in the projection of government policy.

Mr. SPOTILA. Exactly.

Mr. MORAN. Mr. Chairman, I'd like to ask of the three other witnesses your expectation and recommendations with regard to the issue of whether this commission should deal with State legislation in terms of a Federal floor and what the downside of doing that would be. Of course, the other alternative is to simply preempt State legislation with Federal legislation and there is precedent for doing both.

Maybe we can ask Mr. Veator and then Mr. Hatch and Mr. Stone.

Mr. VEATOR. Thank you, Congressman. We obviously generally do not like to have our efforts preempted. On the other hand, I think that is one of the issues that the committee will have to look at as to whether or not preemption, whether it is a floor or overall preemption, should be applied differently to different levels—excuse me different areas. To the extent that we are talking about criminal statutes, that is traditionally within the police powers of the State, then you may not want to preempt those kinds of things.

On the other hand, financial services seem to be increasingly, national if not international, so some level of preemption may be more appealing. Oddly enough, health care and health information, insurance companies that provide or pay for health care generally are still licensed on a State-by-State basis, so it may make sense for States to retain the ability to legislate in those areas.

Mr. MORAN. Would you narrow the scope of the commission to what States—other State studies have done? Have you considered that?

Mr. VEATOR. I don't—at some point, obviously, the commission would want to figure out what needs to be looked at, because as I think one of the witnesses said, privacy is pervasive in every area and the things you keep hearing, again, are financial services, health, identity theft, personal security, that is sometimes threatened by the dissemination of our information. I'm not so sure that the commission needs to narrow its inquiry. In fact, I think one of the things that the commission would have to do is see how all areas of privacy are becoming increasingly related as industry converges as we go on-line and information becomes more and more available.

Mr. MORAN. Thank you. Mr. Hatch.

Mr. HATCH. Sir, I think that certainly with the Internet you're dealing more with interstate commerce, and I think a Federal approach to it would probably be best. With regard to banks, insurance, the type of issues that have—medical, I think the States certainly ought to be able to exercise their police power. Once again, I'm not excited about the idea of a commission. I just have bad vibrations about it, and in the sense that I'm afraid that it's going to be used just to delay action by policymakers.

And for what it's worth in terms of coming up with consistent principles, I would recommend to Congress to look to the restatement of torts on privacy. I mean, it has a very long-debated, researched application of the law. The problem is it doesn't—they have great principles, but nobody ever anticipated the change in technology in terms of the speed with which information is ex-

changed. But the principles are still the same. It is a balance: your expectation of privacy versus the right to know.

Mr. MORAN. That's the point we make that things are happening so fast that self-regulatory capacity seems to be developing. Mr. Stone.

Mr. STONE. Thank you, Mr. Moran. I think that while the concept of a Federal floor and individual State regulation or legislation has some appeal, I think what we are going to be left with is the same patchwork quilt of legislative and regulatory requirements that we currently run the risk of facing today. And as the chairman mentioned a few moments ago, one of the issues that we have to deal with is where do you set the standard for Federal preemption?

I think it is important to recognize that what we are talking about here, at least from the perspective that we are here today, is first and foremost people and their health. And there is no standard essentially high enough that could be set in protecting that.

On the other side of the coin, though, we've heard that we have 2,000 to 3,000 pending privacy bills in State legislatures, which makes my blood run cold in terms of trying to provide services on a national basis. If you're an employer, like a Federal Express with employees in all 50 States, Puerto Rico, and in the District, and you want to provide a proven, comprehensive health program to those employees, if you run into the situation where you're able to do that in one jurisdiction but not able to do that in another, there are obviously some real problems.

I think 50 years ago, health care was very local. You had a local physician, you had a local hospital, you never went outside of town, maybe to the nearest big city for your health care. I don't think that's true today. I think if any of you gentlemen found yourself in need of hospitalization or health care services here in the District, you would like that institution and those caregivers to be able to communicate with your caregivers in your home States. And it is not atypical today for people to travel many States away for health care and for us to be dealing with, because of technology and just because of the aggregation of services, a provision of services from people in States different than where the patient may reside.

I suggest that that is a pretty good picture of what the framers had in mind when they were talking about interstate commerce, and I don't think that it is true today as it was several years ago that health care is entirely local and constrained within the boundaries of the State in which the patient may reside or in which they may be living at the time that they're receiving care.

So I would urge, again, for consideration of Federal preemption, set the standard as high as consensus of you and your colleagues will allow to protect both the rights of privacy, the need for confidentiality and the ability to provide services to the people of America.

Mr. MORAN. Thank you. Thank you, Mr. Chairman.

Mr. HORN. I thank you, and will now go at a few other questions that are somewhat generalist. Mr. Spotila, the thought is that in view of the recent attack on the Federal computer systems, what is the Office of Management and Budget doing to ensure the security of the personal information that is stored on government com-

puters? And obviously that is a major problem. We can do all the legislating we want to have privacy, but if somebody can get access regardless of that, what are the plans in that area the administration has?

Mr. SPOTILA. We have been giving this area priority for some time now. And let me begin by saying that although we are greatly committed to this, and are of the belief that we currently offer good protection to that data, we also understand that the security threat is an ongoing challenge and that there is never a final answer here; that there is a need to continue to maintain and upgrade security as one goes forward in light of changes in technology and changes in the possible threat.

We have been working at the Office of Management and Budget with all of the agencies to improve their approach to information security. We have put out best practices and sets of principles. We have integrated the need to consider information security planning into their information technology planning in the budget process. There was significant improvement last year and the Director this year has given new guidance to the agencies so that this will be rolled into the budget process from the very beginning, going forward.

We think that's extremely important. What we have said, that security is not an add-on, and that one must approach information security in an integrated way from the very beginning as technology planning is done, reflects the best advice of GAO and certainly our best thinking as well.

We are working, in addition to that, with our security agencies, with the law enforcement agencies and with the President's advisor on counterterrorism so that we can support initiatives in that area.

This will be an ongoing challenge, and we certainly look forward to working with you and this committee as we go forward in this area.

Mr. HORN. In your testimony, you mentioned the Health Insurance Portability and Accountability Act of 1996, and you quote Assistant Secretary of Health and Human Services, Margaret Hamburg, as to believing that legislation is the only way to ensure health information privacy.

Has—and that's the bottom of page 4 of your testimony. And the question would be, has the Department explored other alternatives?

Mr. SPOTILA. Well, among other things, the Department is working on finalizing the health privacy regulations that we referred to earlier. It will be issuing a rule this year that we think will be very constructive. We are just concerned that the enforcement powers that are available under existing law are not as effective as they should be and that Federal legislation is needed so that anyone who would misuse personal health information would be subject to accountability. It is really a matter of building on some of the positive steps that have taken place in the past, including these rules that will be coming out this year, and filling in other gaps.

Mr. HORN. Is there any thought as to the type of penalty that might apply at this point?

Mr. SPOTILA. Well, there has been a variety of testimony on what new legislation in this area might look like or what it ought to look

like. We think it is necessary to set the standard correctly first, and then to address penalties. I think that we have to fill the gaps and make it clear that we recognize the sensitivity of health records, that we think that the individual should have some control over how those health records are used and that they shouldn't be used without consent. These principles are vitally important and there are some gaps in terms of how they are applied.

The specific penalty could vary. I think the notion that we've set those standards and that we've tried to address those gaps is the most important principle.

Mr. HORN. Now, has the administration already come up with that in the draft of the Health and Human Services—or do you have other drafts going with the principal idea?

Mr. SPOTILA. There is, as I mentioned, a proposed rule that went out for comment that got 53,000 comments. The Department is working on finalizing that rule. It is a huge task. Reviewing all of those comments and taking them into consideration will be very time consuming. Our timeframe on that is to get the rule out this year. The possibility of future legislation is something that could be looked at.

Mr. HORN. We've got fiscal years, we've got calendar years. Which year?

Mr. SPOTILA. I'm referring to calendar year 2000 for getting the rule out, with the proviso that we would like to do it as soon as it could be done. I don't mean to suggest that it will be the last day of the calendar year.

Mr. HORN. I wanted to know if it was the midnight judges' technique.

Mr. SPOTILA. We would very much like it not to be. Part of a responsible approach to a rule like this is to consider seriously those comments that members of the public made and to take them into account and address in the preamble to the rule what the Department believes about those comments. When you get 53,000, that's a big job. So we are trying to get it right. We are trying also to be fair and proper in the process. So it will be time consuming, but we think the rule will be a good one when it comes out.

Mr. HORN. One of the arguments against developing a new privacy commission is the potential that old work will be duplicated. I just want to ask you if you and your staff and the HHS staff, have they looked at other commission studies at the State level and individuals in Washington think tanks? And what kind of help have you relied on?

Mr. SPOTILA. We have attempted—and the Department, obviously has had the lead here—we have attempted to draw on all of those studies and all of the information that we know of. So that would include those to which you refer. That in going forward in setting up a sensible rule, we could take into account that wisdom.

The comment about the commission or concern about the commission is that it's important that any future effort that studies the privacy area should also build on what has gone before and that should be a guiding principle.

Mr. HORN. Moving to Mr. Veator, in your testimony you mentioned that businesses were taking steps to protect private information. Could you sort of describe the Massachusetts experience and

what is happening in that area and what companies have been successful?

Mr. VEATOR. Well, since finalizing our legislation, we have had the opportunity to meet with a number of businesses who are either happy or concerned at different levels by it, and we have had the opportunity to learn what their privacy protection policies are. And I note that I think that the FTC sweeps Web sites. Web sites with privacy protection policies have gone from something like 14 percent to 56 percent in the last year. So I think more and more companies are aware, especially on-line, that they need have some sort of privacy protection right up front.

Mr. HORN. Now, as I understand it, the Massachusetts Lieutenant Governor has taken an active role in the issue of privacy as a member of the Federal Trade Commission study on privacy. So you found that to be helpful, I take it?

Mr. VEATOR. I think it was both helpful and informative as to how a commission approach really could be very helpful. The particular FTC committee was on providing consumers with access to their personal data on-line and ensuring security of that data at the same time. The committee managed to get 40 representatives, approximately, from industry, privacy advocacy groups, from around the country, and the depth and wealth of information I think that was available in the room when those people met and on lots of conference calls was instrumental in putting together what I think is a very robust analysis of security and access.

Mr. HORN. Mr. Stone, I'm curious; in your testimony you discuss the positive effects on disease management when medical records are accessible to companies such as American Health Ways. Now, beyond the patient's name and the physician's diagnosis, what kind of information do these companies really receive? Is it address, Social Security number, entire medical history or what?

Mr. STONE. Mr. Chairman, it's the entire medical history, both past and going forward, that is received and used by a disease management organization. I think that recognizing we are dealing with a chronic disease population, it's problematic to think of the use of information in an episode-of-care kind of fashion that permeates so much of American medicine. In order to help people with chronic diseases who are ill from the day they're diagnosed and until the day that they die, we need to know how to work with them and their physicians in order to develop and implement care plans that are responsive to the changes in their condition over time.

So we start out with a complete medical record consisting of claims information, the insurance company; pharmacy information, the pharmacy benefits manager; lab information and any information which we can get—which proves to be difficult sometimes because physicians are still pretty much on paper processes in their office—and information from the patient. As this information is updated over time, the patient's stratification within the system will change and the interventions which are provided in support of their self-management efforts and in support of their physician's care plans will change as well.

So it becomes a rather comprehensive clinical and financial database of information with respect to each of the patients that are in the program.

Mr. HORN. Mr. Stone, are there other companies such as yours?

Mr. STONE. Yes, sir, there are.

Mr. HORN. How many are we talking about?

Mr. STONE. Well, the current count is somewhere around 170. I would suggest that a number of those organizations, however, are claiming to provide disease management services in order to take advantage of some of the protections that have been afforded them under the HHS proposed regulations and which were even included in Senator Jeffords' bill on privacy which did not emerge from committee last year. And one of the things that we hope that Congress and/or this commission can do is begin to draw the distinction between those disease management efforts which are legitimately aimed at improving individuals' health and those that are masquerading as a way to offer that chronically ill population something for sale.

Mr. HORN. So disease management would be a generic term, then, for describing the 170; is that correct?

Mr. STONE. Yes, Mr. Chairman.

Mr. HORN. Do you know of any examples where other firms than your own have violated a commonsense standard of privacy?

Mr. STONE. I can't say specifically. I think that if the committee were to look at the broad variety of organizations that are claiming to provide disease management services, and the broad variety of the scope of services that are being offered, staff might very quickly be able to identify segments of the disease management industry that might fall into that category.

Mr. HORN. Let me ask you this. We have in this country a traditional checks-and-balance system, and on the health side you have got outside company inspections. And groups that do this are Veterans Administration, hospital consultants, and so forth. And what other balances do you see to try and keep privacy sacred, if you will, if the individual wants that?

Mr. STONE. Well, if I understand your question correctly, Mr. Chairman, I think that it's important to recognize that disease management as a concept is only 6 or 7 years old, and has made significant strides toward professionalization and self-regulation over the last year to 18 months. I fully anticipate that within the next year to 18 months, we are going to see emerge accrediting programs for disease management organizations. I know that such programs are under consideration by the Joint Commission on Accreditation of Health Care Organizations, URAC and NCQA, among others, and I think those are going to come into play in the relatively near future. I think clearly that kind of good housekeeping seal of approval will go a long way to assuring patients and physicians and health plans that the information being received by organizations with that kind of accreditation has met a certain set of standards.

In the interim, the industry has—is working on its own statement through the Disease Management Association of America on privacy, on the minimum standards that should be in place, and I think that we are going to see not only the accreditation process

develop but a rapid shrinking of the number of organizations offering disease management services as those industry efforts for self-regulation take hold.

Mr. HORN. Now, remind me on that. In your testimony it seems to me there is real concern about State privacy laws that inhibit people from getting the treatment they need. How serious a situation is that and should that be Federal preemption?

Mr. STONE. Well, I think, fortunately, the States have been relatively slow to the legislative process. There is State law in California which was passed at the 11th hour in their last legislative session which is currently going under emergency remediation because of the essentially chilling impact it had on the delivery of disease management service.

I think everybody is familiar with the effort in the State of Maine last year which, while well-intentioned, prevented clergy from visiting people in the hospital because the hospital couldn't tell the clergyman whether the patient was actually there.

Mr. HORN. I thought the flowers example was particularly upsetting.

Mr. STONE. Massachusetts has legislation pending. Texas has legislation pending. Florida has legislation pending. Certainly three bellwether States in terms of health care regulation.

All of which was modeled after the California bill which managed to pass, and the industry association is also lobbying hard in all of those States, pointing out that the California bill is about to be repealed, at least as it relates to disease management.

I think that to the extent that the organizations who are providing these services on behalf of health plans, their members and physicians recognized, again, that this is people's health we are talking about, the issues become fairly straightforward. It's when you fall over the line into the provision of health care services or would-be provision of health care services in support of commerce or some other product or service that the abuses that we've all heard about come to pass.

Mr. HORN. Attorney General Hatch, does Minnesota have a Freedom of Information Act?

Mr. HATCH. Yes, sir, we call it the Data Practices Act; but yes, sir.

Mr. HORN. Has the impact of privacy laws—or would it be, in your mind—in any way change the Freedom of Information Act or would the State have to change it if they had a privacy law?

Mr. HATCH. No, sir. We took—at least the way we're approaching it is we take one segment of society, take it issue by issue: banking, financial data, versus health data versus government data. And oddly enough in Minnesota and I think most States and certainly in the Federal Government, the issue of government data has been with the Freedom of Information Act and the Data Practices Act has been debated and there are statutes in place. There is some effect on government data in Minnesota with regard to the Shelby amendment on driver's licenses. We are having a debate on that issue. But pretty much government information is leaving it alone in terms of what the Data Practices Act contains, which parallels very closely what goes on at the Federal level.

Mr. HORN. Well, let's hear about the Federal level. Mr. Spotila, how much, if any, would be a problem with, say, the HHS privacy regulations which are out there now and the Freedom of Information Act? Is there a problem there, and has anybody between Justice and your office thought through those problems?

Mr. SPOTILA. Our sense is that there is not a problem, that the Freedom of Information Act has always allowed for the protection of private information of the sort that we are talking about, individual information.

In terms of what the HHS rule will look like as a final rule, that is still in the course of development. We're certainly sensitive to not creating a problem with the Freedom of Information Act; that would be something that we are always going to be careful about.

Mr. HORN. Do any of you see any problems here that we haven't brought up yet that you'd like to raise and maybe did not raise in your own statements? Do you have something, Mr. Spotila?

Mr. SPOTILA. Nothing else, other than as I mentioned, that we welcome the good intentions that are reflected in this bill and would look forward to working with the committee further.

Mr. HORN. Getting back to Mr. Hatch a minute, in your testimony you talked about the need for the States to take action on the issue of privacy. Our staff has talked with people from the Mayo Clinic and the University of Minnesota. They discussed their concerns with privacy legislation initiated in the Minnesota legislature saying the opt-in policy was not successful for them.

Mr. HATCH. Sir, what that relates to is it is a separate bill. In Minnesota, health data is transferred to the government without your permission; all patients without permission, without knowledge. And what I proposed is a bill saying at least you ought to get the consent of the patient. Center for Disease Control, Mayo Clinic and everybody else does it.

I am surprised that all of the health information, at least health data is being transferred to the Minnesota Department of Health Data Institute without even the knowledge of the patients, and there are a number of issues that will be coming out with regard to how that information is being used.

In that case, there were physicians at the Mayo Clinic who were on the Health Data Institute who opposed it even though only 60 percent of the—a little more than 60 percent of the patient data that is being sent, again without knowledge, people who are charity cases, people who pay cash, people that go in for certain types of, say, cosmetic surgery surgeries that are not covered by an HMO or insurer, are not transferred. So actually, statistically, the information is not as credible as a process where you do get the consent of a patient, simply because 97 percent of them will consent to it. In this case it is about 60.

I don't oppose having the information sent to the government as long as you don't have a patient's name and Social Security number attached to it. And there have been examples of leaks; you mentioned yourself, sir, with regard to government data being transmitted inadvertently. We had examples in Florida of lists and certainly we have other statutes that require listing of epidemics—epidemiology with regard to transferable diseases. But they did dis-

agree with the idea that the patient ought to have to give consent because their data is being sent.

Mr. HORN. Has there been any effect on the quality of medical research to your knowledge?

Mr. HATCH. No.

Mr. HORN. Here people would argue the Shelby amendment is a problem.

Mr. HATCH. Your Honor, in Minnesota the Department of Health has never issued any studies. They gather the data but no studies have ever been issued. And, indeed, if they did, given the fact that only 60 percent of the data is being transmitted, it is probably less credible than the research facilities that do get patient consent. They get about 97 percent data response.

My beef with that is simply that you ought to at least notify the patient. When you walk into a hospital you have to sign three times. One of them is a consent form that basically allows a transmission. It seems to me before it goes to the government, there ought to be some acknowledgment by the patient that it goes. Either that, or you can send the data, but just don't send the patient's name with it. Give it a code. That was my beef.

Mr. HORN. In other words, your State health department could collect this data but would not need to have the address and the name of the person that is the result of that data?

Mr. HATCH. Sir, yes, and my proposal did not pass. So that's the one that did not get enacted.

Mr. HORN. How about it, Mr. Stone? How much of a difficulty would that be with, say, the management—disease managment companies?

Mr. STONE. I think, Mr. Chairman, there are significant differences between research which requires aggregated data but does not require, as General Hatch suggested, patient names and identifiable information for the analysis on that data to be carried out, and for activities that are in the stream of delivering health care services, which is where our industry, our company, HHS, Senator Frist and Breaux and the President have all put disease management as part of the treatment side of medicine.

And to do treatment effectively, you need to know who you are talking to and where they live and how to contact them so that you can have intermittent actions, whether those be face to face, phone, Internet or whatever, with those individuals in order to further their care.

Mr. HORN. But does the patient know that this personal information is being released to you?

Mr. STONE. I would say probably not, since in our case, anyway, all of our programs are private labeled for the insurer who is our customer. So the patients and their physicians are advised of a new diabetes program for Cigna Health Care. The patients are given an opportunity, in our model specifically, to opt out of participating in that program. Less than 2 percent do. And if they don't, they begin to receive interactions as if our personnel were Cigna's personnel. So I doubt that they know that it's coming from American Health Ways.

Mr. HORN. Now, you operate in all 50 States or what?

Mr. STONE. We're currently operating, I think, in 33 States.

Mr. HORN. In 33 States; is there any way that employers, insurance companies, could get those lists of yours with, say, diabetes or cancer or whatever?

Mr. STONE. Other than the insurance company that we are providing the program for? I guess there is, given the ability to tap into electronic data systems. But it would be extremely difficult since we are not using the Internet, we are operating on a closed network at the moment and we are transferring information back and forth with our insurance plan customers on a weekly or monthly basis.

Mr. HORN. Well, what kind of data could you find in a small Minnesota town, let's say, where you have got 200 people and Olie is 57 years of age, you don't need his name, everybody in town knows he's 57. Isn't that a worry for you? I think it is for a lot of people who say, gee, the boss is going to hear that I've got this disease and there goes my pension.

Mr. STONE. I think that the issue you're raising Mr. Chairman, is a very real issue. Most of the companies that we have talked to do not want to know, and create some very serious iron walls between their H.R. functions as it relates to their employees and those individuals in the organization who may have personal health care information and the review, hiring, firing processes of the company.

We do not provide information back to an individual's employer. Our exchange is strictly limited to the health plan that has hired us to work with their members and their providers for the delivery of disease management services. So it is a very tight network.

Mr. HORN. Well, could that health plan just cancel them like that? I find health plans aren't exactly easy to deal with.

Mr. STONE. Without meaning to, obviously, to step on our customers' toes, again, I guess that's certainly possible. I think what's happened in the health plan industry—and I would, you know, defer to their industry association for more detailed response—that they have recognized finally that the days of riding the utilization review and contracting horses to margin are over. And with somewhere between 10 and 15 percent of all their members having chronic diseases, with all of us getting older, and therefore sicker, health plans have begun to realize that if they are going to ever return to any kind of reasonable margin level, they are going to have to take care of patients. And the basic premise underlying all disease management is that healthy people cost less.

Mr. HORN. Now, you work with university medical researchers on a lot of your work?

Mr. STONE. No, we don't.

Mr. HORN. You don't?

Mr. STONE. No.

Mr. HORN. So there aren't any studies being done, then, as to the success or not success?

Mr. STONE. Well, in fact, there are. In 1998, there was a study released by the Lewin Group, Dr. Rubin was the principal author, former assistant Secretary of HHS, which validated our outcomes for our diabetes program for 7,000 commercial members in HMOs. And as I alluded to in my testimony, next week we will be releas-

ing a similar study on 20,000 HMO members in Medicare-Plus Choice plans.

So despite the fact that we are a commercial venture, we are fully prepared and have always been prepared to put our results out there to stand the scrutiny of public and scientific review, and in the hope that people will come to recognize that these kinds of programs do improve health, do create satisfied consumers and providers and save significant amounts of money.

Mr. HORN. Let me round that one out. When an organization or a company such as yours or other types in medical research receive public money for, say, research, does the taxpayers or the government at all levels have access to private records used in a publicly funded study? I would be interested in what you all think on that one.

Mr. STONE. I don't know that I have the expertise to respond to that. I do know that 2 years ago we entered into an agreement with NIH to provide them with blinded aggregate data from our database. And it is now the largest single database on diabetes in the country. NIH was perfectly happy to take that data in a blinded format without any patient identifiers on it. Although I have to admit in 2 years they have never once asked us for anything.

Mr. HORN. Mr. Hatch.

Mr. HATCH. The issue I was going to advise in private practice as a lawyer—I represented insurance companies and third-party administrators as well as some patients, actually, but the third-party administrators of self-insured plans all—I shouldn't say all, but most at one time or another do get a request from an employer with regard to issues concerning health care. They were uniformly advised you have ADA issues here; don't recommend that you be doing this. On the other hand they are telling me: That is easy for to you say, but that is my largest client.

And I recall vividly, one being a trucking company, requests the copies of anyone having chemical dependencies. The issues here—this is the other side of it. The public, if you're a patient and you're aware that that data is going to be transmitted beyond the doctor, you won't get treatment. I will not go in for chemical dependency treatment if I know that my employer will find out. Or as an Attorney General, if the voters would find out, maybe it is something that I want to keep confidential.

Too many areas, venereal diseases, there are too many issues that crop up in our lives. But if I know that that is being transmitted, that is going to interfere with the physician's ability to treat the patient.

And I don't have any problem with aggregate data, even with patient identifier data if the patient signs off, gives a consent. And my understanding is that roughly 97 percent of the public will give consent on that, at least participated in that decision.

Mr. HORN. Mr. Veator.

Mr. VEATOR. We currently have a bill in front of the Massachusetts Legislature relating to just that question. And I think the issues have come down to the same, which is how do you ensure or motivate the use of aggregated, deidentified data, and then how do you protect people who want medical services and at the same time are aware that either through sharing information by insur-

ance companies between either health care insurers or life insurers, how you get medical services when they're worried about that data being disseminated, properly, as it turns out in many cases. Those are the issues I know that the Massachusetts Legislature is dealing with now.

Mr. HORN. In your research on that, in Massachusetts, are there a number of States doing the same thing?

Mr. VEATOR. I think so. I know that California, for example, has either enacted or has something pending along those lines.

Mr. HORN. Let me ask you, Mr. Spotila, what's the Federal Government's position on this?

Mr. SPOTILA. There are two aspects I would point out. Aside from this issue of aggregate data versus treatment information, we are also aware that the Centers for Disease Control and perhaps other public health agencies might have access to information about medical conditions. But they have handled that information in accordance with the Privacy Act and other confidentiality restrictions. There's always a need for balance between proper use and privacy.

The proposed rule that the Department of Health and Human Services has put out on health privacy also deals with this subject. We are likely to see an addressing of it in the final rule either through the setting of criteria or insistence that the identification tags be removed from some of that information.

It's an important question. It's very much on everyone's mind, and we are trying to strike the right balance to make certain that we don't lose some of the advantages, whether it be improved treatment or public health response, as we take better steps to protect individual privacy.

Mr. HORN. Let me move back to Attorney General Hatch now. In your testimony, you mentioned how you took legal action against the U.S. bank for selling personal information to marketing companies such as Member Works Incorporated. I'm curious, what additional actions did the Minnesota courts take to protect the interests in personal privacy?

Mr. HATCH. The courts or the legislature? The courts?

Mr. HORN. The courts.

Mr. HATCH. Well, both cases settled, so they did not go any further than that. I think there's still a class action that's pending in the private side of it.

In the U.S. bank case, the bank did agree to prohibit—to not agree to any distribution even with consent, basically. They cannot distribute information to third-party marketers. They can distribute to affiliates on an opt-out. So it is—oddly enough, that bank is probably working under stricter guidelines than any other bank in the country right now.

The Member Works we did settle. The allegation there was essentially they took the data, including the date of birth, and basically according to the audiotapes of the supposed consent, our estimate is roughly half never agreed to any acquisition. While we did not have statistics on it, I was surprised at the age of people; it could be that they're the only ones home that are answering the phones; could be they are the ones that are most vulnerable to a direct sales pitch. But it may also be that companies are targeting that group, and I don't know. But we will have more knowledge on

that I think by year end as we're gathering through it and looking at other cases.

But it appears that, you know, the financial data, two-thirds of fraud basically is directed against senior citizens, No. 1, because they've got the money, it is their nest egg; and No. 2, they are perhaps more trusting, more vulnerable.

And financial data in the wrong hands is very—can be very dangerous. And the courts have not gone further, but other than that, we do have class actions pending.

Mr. HORN. We have another few hours this week, not for your panel, but for the panel on Tuesday and we will set up another panel, panels one and two, on the Tuesday one, and then we will have a hearing later in the week on a related subject, which involves Social Security in relation to privacy and the numbers thereof.

So what I'm going to do today is just thank you all, because you have given us a number of vital perspectives that we really need, and we hadn't thought about. So I am most grateful to you for the testimony you have given to us.

And I do want to thank the staff for putting this together and that is J. Russell George, the staff director and chief counsel for the Government Management, Information, and Technology Subcommittee; and then on my left, your right, Heather Bailey is the counsel for this hearing. Bonnie Heald, director of communications back there next to Mr. George; Bryan Sisk, the clerk; and Liz Seong, is an intern; and Michael Soon, intern. And then Trey Henderson is counsel for Mr. Turner, the ranking member, and the minority; Jean Gosa is minority clerk. And we have today Doreen Dotzler and Joe Strickland as the court reporters.

And I will now read the statement from the Attorney General of the State of Texas and put that in the record.

I don't know if the Attorney General is Democrat or Republican. You might know.

Mr. HATCH. He's a Republican.

Mr. HORN. He's a Republican, OK. Because I know the Governor has a lot of Democrats in the State government, so I did not quite know whether this was one of the Republicans that got in. But his letter is very interesting. He said—this is John Cornyn, Attorney General of Texas. He says:

I want to express my support for the privacy commission, H.R. 4049, under consideration by our committee here. And this legislation proposes the creation of a privacy commission that will undertake a comprehensive study of the issues relating to the protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing appropriate uses of information.

With the advent of the Internet and the information era, privacy has become a central issue for American citizens, industry and policymakers. As consumers are becoming more aware of the personal information that is being collected and used by on-line companies, their concern about individual privacy is growing.

The technology industry is also focused on the privacy issue. Recognizing that the future of the Internet depends on consumer confidence, the technology community has taken laudable steps to develop self-regulatory standing programs to build consumer trust in the new medium. The erosion of the consumer trust poses a serious threat to personal privacy and the future success of e-commerce and thus creates the need for government to consider appropriate steps for the protection of consumer privacy.

At the same time, however we must find a way to protect consumer privacy without stifling growth and innovation in the rapidly changing world of cyberspace. I

believe the establishment of this commission is a step in the right direction toward achieving this balance.

Over the past few years, privacy initiatives have cropped up across the country. The Federal Government, States, the private sector, industry groups, and consumer groups have all formed working groups to study the issue. None of these initiatives, however, appear to be taking the coordinated global approach proposed by the Privacy Commission Act.

Because the Internet has no boundaries, it is imperative that Federal, State and local efforts to protect privacy and encourage the growth of the new economy be coordinated. Government, industry and consumer groups need to work together to help define their appropriate roles in achieving a balanced solution to the privacy problem. State attorneys general have a unique perspective to share in this debate because we are responsible for protecting consumers' rights in 50 States.

As the Attorney General of Texas, I am deeply concerned about the privacy issue. In particular, I am concerned about protecting children's privacy and maintaining the confidentiality of sensitive medical and financial information. In Texas, we are currently studying our laws to determine how we can best protect consumer privacy while still encouraging the growth of e-commerce.

My office has created an Internet bureau that will protect consumers' privacy online in addition to fighting cybercrime. Over the last month, I have met with numerous members of our very large and growing technology community in Texas. I have gained an understanding of the industry's concerns and its efforts to regulate itself in the privacy arena. In Texas, we are working to protect consumers while fostering the growth of technology businesses.

Because I believe the proposed privacy commission will help coordinate the efforts and perspectives of all of us involved in the privacy debate, I encourage your subcommittee to support the proposed Privacy Commission Act.

Thank you for your consideration of my views. I respectfully request this letter be submitted for the record.

We thank you; and we thank Attorney General Hatch; and we thank you, Mr. Veator, on the State perspective; and we thank you, Mr. Stone, on the very interesting and unique model that is going on in disease management. And we thank you, Mr. Spotila, for giving us the broad view of what is going on in the Federal Government. Thank you very much for coming.

Now, the Democratic staff and the Republican staff might have additional questions, and if you don't mind we would like you to respond to them because Mr. Turner had to go out for a very important meeting. He might well have some questions, and we would appreciate it if you would give those answers. We will put them in the record without objection at this point.

At this point, we are recessing until Tuesday at 2 p.m. to continue the rest of the panels, and that is in room 2247. The full committee, I believe, is in here. It will be in room 2154. The full committee is not meeting.

With that, we are adjourned.

[Whereupon, at 4:03 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Statement by

Willis H. Ware

To the

Committee on Government Reform
Subcommittee on Government Management

United State House of Representatives

Hearing On

Establishing a Commission for the Comprehensive Study of Privacy Protection

HR 4049

May 15, 2000

Introduction

Mr. Chairman and members of the Subcommittee, I regret not being able to be present in person today to discuss a topic which has been a central item of both my personal and professional attention for the last 30 years. My name is Willis H. Ware and I have enjoyed a lifelong career with the RAND Corporation of Santa Monica, California. My present status is that of resident consultant and staff member emeritus; but in the past, I have held various management and research staff positions within RAND. In these several roles, I have participated in many policy studies, both within the company and as member or chairman of various federal-level committees and advisory boards.

The views presented below are personal ones that reflect my fifty years in the computer field; and of that, thirty years have included an involvement with privacy, information security, and critical infrastructure protection. My views were formulated without reference to prior testimony before the subcommittee; and to the extent that there is similarity or overlap, it is coincidental. These views are based on my professional achievements and experience; in no way do they reflect any that might be held by RAND

In the early 1970's I chaired [HEW] Secretary Elliot Richardson's committee on Automated Personal Data Systems. This effort produced the well known report: *Records, Computers and the Rights of Citizens*. The work of this group provided the intellectual stimulus and framework for the Privacy Act of 1974. In particular its report introduced the concept of a Code of Fair Information Practices, and provided the details of such a Code. The Act, in turn, established the Privacy Protection Study Commission [PPSC] to which I was appointed as a Commissioner by President Ford; I also served as its vice chairman. I have given many presentations and written many papers on various aspects of personal privacy, many of them addressing policy considerations relevant to actions that the federal government might have taken. My name, reputation and achievements are well known in the fields of information security and personal privacy.

Semantics

Let me caution the subcommittee that the word *privacy* is sometimes used as a synonym for *confidentiality*. HR 4049 uses the word in its proper and original sense; namely, the collection, storage, and use of information about individuals for the purpose of making decisions about them for some right, benefit, or privilege. That is also the sense in which I will use the term today. To put it another way: what personal information will be allowed to be collected, and for what purpose will it be allowed to be used.

Scope of Statement

I will not address the need for Congress to attend to the privacy issue. You have already heard excellent testimony during your April hearings, particularly the statement of Mr. Robert Douglas which illustrates how the Internet is creating serious privacy issues, and the statement of Ms. Sallie Twentyman which describes so poignantly how the growing incidence of identity theft impacts an individual. It goes without saying that the privacy issue is in urgent need of attention.

Neither will I address the detailed wording of the draft bill, although I offer some thoughts for minor adjustments.

I want to concentrate on the larger aspect; namely, the setting in which this bill is presented before Congress, and the expectations that Congress might have from a commission that this bill would create. In providing my views, I have drawn on my experience as a commissioner of the Privacy Protection Study Commission which did a similar study in the middle 1970's, and my experience as chairman of the HEW Committee.

The Present Privacy Issue

I think it important for the subcommittee to understand how the privacy issue has evolved. During the HEW Committee work, the focal point of concern was the government agency, and its holdings and use of personal information. The federal government was seen as *the* problem. Of primary concern were the huge databanks that federal agencies maintain in support of their missions. There was also an overtone of instituting a universal personal identifier which Congress was considering; namely, the Social Security Number. During the work of the Privacy Protection Study Commission, the scope of privacy concerns expanded to include the behavior of large corporations. They also operate large recordkeeping systems and data banks of personal information which has been gathered primarily to support the corporate mission and its marketed products and services.

In the intervening 25 years, the new and present concern is the information industry per se -- an industry in which information about people is gathered solely to become a commodity and a marketable product. As well understood and underscored by your prior testimony, the very existence of the Internet has been a major driver in the emergence of this new aspect. And of course, the older aspects of privacy have become more complicated and complex under the widespread adoption of electronic computer and communications technology; e.g., the electronic delivery of benefits such as food stamps, the electronic filing of tax returns and other documents, electronic commerce.

Admittedly, the three different aspects of the privacy issue do not exist in individual isolation; they do indeed interact. But for the work of the Congress it is important to understand the evolving structure of the privacy issue, and which aspects have some coverage in law vs. those that are completely unaddressed. I think that Congress, and any new commission, would find that extant privacy laws probably are in need of some updating to reflect the contemporary information infrastructure.

Detailed Comments

1. I have no comment on Section 2, Findings. The statements therein are in the nature of scene setting, are generally satisfactory, and sufficient for establishing the thrust of the bill.

2. One comment on Section 3, *Duties of the Commission*. This levies an appropriate charge on the Commission except that it is worded as though the privacy issue had never been studied before. There is no reference to the many studies that have been done, in particular the PPSC effort of the mid-1970's. If it is appropriate for a law to reference precedence and history of an issue, I would think it proper to modify this section accordingly. Certainly, a new and wise commission would first read thoroughly the PPSC report, the intervening other studies, and determine what had changed and how. A new commission would have to decide which privacy issues

need to be addressed de novo; and which simply need an update or possibly extrapolation.

3. Membership. Seventeen is a big group; the PPSC had 7 members. After the death of one, the bulk of its work was done by the remaining, supported by a very effective staff. The enabling act provided that two members would be from Congress, which was a consequence of how the Act came into existence. Generally, the PPSC had perfect attendance for its meetings, except that the political members tended to have schedule conflicts, often unexpectedly. High attendance was very important, especially for those discussions in which positions were argued out. On balance, I would say that the bulk of the intellectual insights, and the innovative positions and solutions came from the private sector members of PPSC and from the staff.

In regard to this current effort, I would have great concern that the wording of Section 5 will tempt the Congress to appoint its own with the result that the commission would become a political animal, whereas it must be a thoughtful policy-oriented study group. I would urge that at least half, even 2/3, of the membership be from the private sector and a minimum from within government. The law should make this clear. The reality of getting good commissioners will lie in the selection process, and probably cannot be addressed in words of the law.

I take this position on membership for a very significant reason. In the 1970's, the privacy issue was considered to be a problem driven by the actions of federal agencies. In the 2000's, the privacy problem is driven equally by the government and by the private sector. Indeed, many of HR 4049's findings are issues deriving from the behavior of the private sector. This is all the more reason for a large fraction of a new commission to be non-government people.

4. Section 6 is straightforward. I would observe that the PPSC fortunately had a chairperson who had been through a prior committee action on privacy [HEW Secretary Elliot Richardson's study committee]. Ms. Carole Parsons [Bailey] was experienced, knew the topic very thoroughly, and was a dedicated worker. A law probably cannot address the qualifications of the staff director, but the success of the commission will depend very heavily on the person's qualifications. You would not want someone for whom this would be seen as just another administrative assignment; you would want someone dedicated to the cause and ideally, already knowledgeable about it.

5. Section 7 is largely conventional legislative boiler plate and needs no comment.

6. Section 9. I would estimate that $2.5M is too little for the commission to do a comprehensive job. It is true that past work and the experience of history is much more extensive now than it was in 1975. Therefore, one might suppose that the task of a new commission would be less demanding than that for the PPSC. The PPSC expended (as I recall) $2.25M over 2+ years but just the effects of inflation over 25 years would make a realistic funding more like $4-5M.

In addition I point out that the nature of the privacy issues are today every bit as complex and intricate as they were in 1970 and again in 1975. The new aspects and the recent evolution of privacy are very different from what has been studied before; history and insights are minimal on their particular nature. A current commission would have as difficult a task as did the PPSC, especially given the fast moving nature of the electronic world. Thus, one should not expect a new commission to do its task (so to speak) "on the cheap"; it must be adequately funded and certainly more generously than the draft bill provides.

Overall Time Line

I want to estimate the likely time line for a new commission because it relates to the Congressional expectations for and from it. HR 4049 is just starting through the legislative process. With luck it might be signed into law before the present Administration changes. It would take perhaps 6 months or so before funding would be available, office space located and arranged for, a director and staff on hand, etc. It could be even longer before all appointees were in place. Allowing for a little slippage, let us suppose that HR 4049 is passed; and the commission, fully functional by the end of 2001.

It is projected to be finished in 18 months thereafter. It probably would take of the order of 4-6 months for the Commission to argue out its position, formulate its recommendations and publish a report. If that were subtracted from the 18 months, that leaves a year or so to do substantive work -- a minimal calendar period. The PPSC functioned for 2 years and 3 months and we had a very intensive schedule for hearings and work, supported by full-time staff activities and interactions with commissioners between meetings. Nonetheless, all that aside; suppose it could happen. A report would then be before Congress sometime in 2003.

Congress and the [then] Administration would have to decide what action to take. Who knows how long that would take, but my guess is that little remedial privacy law could be in place before 2005.

Meanwhile, the private sector world and its electronic infrastructure is moving very rapidly. We all know it. Driven by a seemingly overwhelming urge for economic opportunity and by abundant venture capital, the private information industry and electronic commerce -- the new twists to the privacy issue -- are creating privacy infractions almost faster than they can be identified.

> To wait until 2005 for remedial action on pressing and current privacy issues strikes me as being neglectful of a very important social issue.

Congressional Expectations

Even if my time estimate could be squeezed by a year -- 2004 for legislation or rule

making -- the beneficial consequences are likely to still be marginal. The privacy issues of today will either have been solved, will have become overwhelming and outside the reach of any reasonable law or regulation, or their consequences will have been accepted by society.

I make this major observation.

> I think it is a serious shortfall in outcome if Congress expects the results of a new privacy commission to point the way for the country to handle its present privacy obligations.

I fear that any report of a commission, no matter how excellent, will have been overtaken by events in the real world. There is no way that the commission could be agile enough, especially in its political setting, to keep up with the moving target represented by today's privacy issues.

Alternate Approach

I cannot express pessimistic views about the effectiveness of HR 4049 without offering an alternate choice. I would rather have Congress focus on 2 or 3 of the obvious privacy problems of today and deal with them; but still create the commission as the means to provide a forward looking big picture. The combination of its report plus the experience of the legislation -- that I would hope Congress could pass on 2-3 issues concurrently -- would put the country in position about 2005 or so to review the privacy situation, make adjustments in old legislation, and innovate new.

One can debate what current major privacy issues require attention, some more urgently than others. Certainly, medical and financial privacy are both high on the list, especially the role of the SSN in these areas. Also urgent for attention is the privacy dimension raised by the interaction of commercial interests with the Internet. The activities of the law enforcement community should be on the list. The behavior of the federal government could stand review, as might the actions of the states and their electronic interactions with the federal government. Privacy consequences of the drive to protect the critical infrastructure might be on the list.

In fact, Congress could profitably hold hearings on the question: "What are the major privacy issues that Congress should address in 2001?" Or Congress might request some appropriate study organization to conduct such an examination, perhaps in workshop format to economize on time.

Conclusion

HR 4049 is generally satisfactory as an item of legislation to create a new privacy commission; it could stand some fine tuning as suggested above. My concerns are two

fold:

> Is the calendar period one in which the commission's work could have any consequence for present privacy concerns?
>
> What are the expectations of Congress and can this approach satisfy them? Is the effort worth the while?

In considering these two points, note also the following. In 1970 and again in 1975 when the HEW Committee and the PPSC were respectively in operation, there were no really pressing privacy issues demanding attention. While the privacy issue itself transcended academic interest, the incidence of privacy infractions and personal harm were occasional. There were few events in the real world threatening the citizenry in a major way; whatever time the PPSC needed for its task could be easily accommodated without serious risk to the country.

Today is different; everything is happening much faster. Progress is at electronic speeds; the proliferation in usage of modern information technology is astounding. Unlike the situation in 1975, there are many privacy issues demanding attention now; there are many privacy issues threatening the citizen -- even new ones seemingly on an almost daily basis. There are no checks and balances in place to give the citizen standing to seek redress or remedial action in case of harm. Thus, you will understand (a) my concern about the time table over which a new commission could lead to remedial privacy actions and (b) that independent efforts by Congress are needed to address today's privacy threats.

OFFICE OF THE ATTORNEY GENERAL · STATE OF TEXAS
JOHN CORNYN

May 23, 2000
→ Mr. Kaylen
For the hearing record
C.

May 15, 2000

The Honorable Stephen Horn
Chairman, Government Management,
Information & Technology Subcommittee
U.S. House of Representatives
2331 Rayburn House Office Building
Washington, D.C. 20515

Re: Privacy Commission Act

Dear Chairman Horn:

I want to express my support for the Privacy Commission Act (H.R. 4049) currently under consideration by the House Government Reform Committee and your subcommittee. This legislation proposes the creation of a Privacy Commission that will undertake a comprehensive study of the issues relating to the protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing appropriate uses of information.

With the advent of the Internet and the information era, privacy has become a central issue for American citizens, industry and policy makers. As consumers are becoming more aware of the personal information that is being collected and used by online companies, their concern about their individual privacy is growing. The technology industry is also focused on the privacy issue. Recognizing that the future of the Internet depends on consumer confidence, the technology community has taken laudable steps to develop self-regulatory standards programs to build consumer trust in the new medium.

The erosion of consumer trust poses a serious threat to personal privacy and the future success of e-commerce and, thus, creates the need for government to consider appropriate steps for the protection of consumer privacy. At the same time, however, we must find a way to protect consumer privacy without stifling growth and innovation in the rapidly changing world of cyberspace. I believe the establishment of this Commission is a step in the right direction toward achieving this balance.

Over the past few years, privacy initiatives have cropped up across the country. The federal government, states, the private sector, industry groups and consumer groups have all formed working groups to study the issue. None of these initiatives, however, appear to be taking the coordinated, global approach proposed by the Privacy Commission Act. Because the Internet has no boundaries, it is imperative that federal, state and local efforts to protect privacy and encourage the growth of the new economy be coordinated.

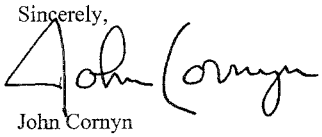
POST OFFICE BOX 12548, AUSTIN, TEXAS 78711-2548 TEL: (512)463-2100 WEB: WWW.OAG.STATE.TX.US
Equal Employment Opportunity Employer · Printed on Recycled Paper

Government, industry and consumer groups need to work together to help define their appropriate roles in achieving a balanced solution to the privacy problem.

State Attorneys General have a unique perspective to share in this debate because we are responsible for protecting consumers' rights in the fifty states. As the Attorney General of Texas, I am deeply concerned about the privacy issue. In particular, I am concerned about protecting children's privacy and maintaining the confidentiality of sensitive medical and financial information. In Texas, we are currently studying our laws to determine how we can best protect consumer privacy while still encouraging the growth of e-commerce. My office is creating an InterNet Bureau that will protect consumers' privacy online in addition to fighting cybercrime. Over the last month, I have met with numerous members of our very large and growing technology community in Texas. I have gained an understanding of the industry's concerns and its efforts to regulate itself in the privacy arena. In Texas, we are working together to protect consumers while fostering the growth of technology businesses.

Because I believe the proposed Privacy Commission will help to coordinate the efforts and perspectives of all of us involved in the privacy debate, I encourage your Subcommittee to support the proposed Privacy Commission Act. Thank you for your consideration of my views. I respectfully request that this letter be submitted for the record.

Sincerely,



John Cornyn
Attorney General of Texas

JC:cm

cc: Congressman Judy Biggert, Vice Chairman
Congressman Thomas M. Davis
Congressman Greg Walden
Congressman Doug Ose
Congressman Paul Ryan
Congressman Jim Turner
Congressman Paul E. Kanjorski
Congressman Major R. Owens
Congressman Patsy T. Mink
Congressman Carolyn B. Maloney
Texas Delegation

H.R. 4049, TO ESTABLISH THE COMMISSION FOR COMPREHENSIVE STUDY OF PRIVACY PROTECTION

TUESDAY, MAY 16, 2000

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

The subcommittee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Turner, and Waxman (ex officio).

Also present: Representatives Hutchinson and Moran of Virginia.

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

Mr. HORN. A quorum is present. We have a vote on the floor, and we will be in recess until 20 after 2. We're in recess.

[Recess.]

Mr. HORN. A quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will resume.

The subcommittee is continuing its examination of H.R. 4049, a bill to establish a commission on the comprehensive study of privacy protection.

Yesterday the Honorable John Spotila, Administrator of Regulatory Affairs at the Office of Management and Budget, testified about the efforts being taken by Federal agencies to protect private information against inappropriate disclosure.

Minnesota's Attorney General Mike Hatch and Mr. David Veator, from the Massachusetts' Office of Consumer Affairs and Business Regulation discussed the complexities of attempting to craft appropriate State legislation.

Our fourth witness was from the private sector and discussed why such legislation is necessary. Mr. Robert Stone is the executive vice president of American Healthways, a company that provides disease management programs to about 170,000 people enrolled in health maintenance organizations. His company sets up treatment plans for patients with chronic illnesses. Mr. Stone testified that in

many States HMOs share their patients' medical records with disease management companies such as American Healthways, even though most patients are unaware that a third party is viewing their personal records.

With that, we will proceed with the panels today, and we will begin with panel one for Tuesday. Mr. Belair I see is here, editor of Privacy & American Business; Dr. Mary Culnan, professor, McDonough School of Business, Georgetown University; Christine Varney, former Commissioner, Federal Trade Commission; and Solveig Singleton, Director of Information Studies at the CATO Institute; Ron Plesser, legislative counsel, 1977 Privacy Commission, and Stanley Sokul, member of the Advisory Commission on Electronic Commerce.

Let me explain how the subcommittee works. We work essentially that once—we're going right down the line, and your statement is fully put in the record. We'd like you to summarize it in 5 minutes so we can have a dialog between the Members here and the other witnesses so we get something from that besides simply a written paper. In the case of government agencies, usually the person's never written the paper, but you're different, and I know you struggled over it probably like all of us when we are in the private sector.

So we will also have panel two today, the Honorable Edward Markey, Member from Massachusetts; the Honorable Joe Barton, Member from Texas; the Honorable Jim Greenwood, Member from Pennsylvania, and they will join us on panel two.

So we think we are without a lot of votes to disrupt us today, but that's democracy, so we have to do that. It's always a pleasure to take a walk anyhow around here.

[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
[illegible] L. MICA, FLORIDA
[illegible] AS M. DAVIS III, VIRGINIA
J.M. McINTOSH, INDIANA
[illegible] 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
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

Subcommittee on Government Management, Information, and Technology

"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
May 16, 2000

A quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will resume. The subcommittee is continuing its examination of H.R. 4049, a bill to establish a commission on the comprehensive study of privacy protection.

Yesterday, the Honorable John Spotila, Administrator of Regulatory Affairs at the Office of Management and Budget testified about the efforts being taken by federal agencies to protect private information against inappropriate disclosure.

Minnesota's Attorney General Mike Hatch and Mr. David Veator from Massachusetts' Office of Consumer Affairs and Business Regulation discussed the complexities of attempting to craft appropriate state legislation.

Our fourth witness was from the private sector, and discussed why such legislation is necessary. Mr. Robert Stone is Executive Vice President of American Healthways, a company that provides disease management programs to about 170,000 people enrolled in health maintenance organizations. His company sets up treatment plans for patients with chronic illnesses.

Mr. Stone testified that in many states HMOs share their patients' medical records with disease management companies, such as American Healthways, even though most patients are unaware that a third party is viewing their personal records.

American Healthways does not share the medical records with other companies, such as marketing agencies or employers, Mr. Stone said, adding that not all of the 170 companies that provide similar medical services are as respectful of patient privacy.

Today, the subcommittee will continue this important discussion with representatives from privacy commissions that have been established by state and federal agencies. They will discuss their work, and suggest areas that need additional study.

I welcome our witnesses, and look forward to their testimony.

Mr. HORN. So we will begin, then, with, besides my opening statement, I believe the gentleman, the ranking member on the full committee, Mr. Waxman for an opening statement.

Mr. WAXMAN. Thank you very much, Mr. Chairman. I want to commend you for holding hearings today and yesterday on H.R. 4049. I regret I was unable to attend yesterday's session due to a preexisting schedule conflict. I was flying back from Los Angeles. You know how that is, Mr. Chairman. But I understand the session was informative.

H.R. 4049 proposes a $2.5 million privacy commission to study a wide range of very complex issues that affect a tremendous number of stakeholders. It is important to examine this proposal carefully and ensure that those with relevant expertise and experience have had a chance to review it, and I appreciate that you facilitated that process with this week's hearings.

The schedule the subcommittee has set for moving this legislation forward, however, may be self-defeating. Many of us want strong privacy legislation, but the rushing pace we are following with this bill may result in legislation that is counterproductive to privacy efforts. H.R. 4049 was introduced at the end of March. The subcommittee announced last week that it is interested in having a markup by next week. This intention to mark up this bill by next week was announced before the subcommittee even heard from the many experts that are coming before us this week, and as we saw from testimony and statements provided yesterday, the bill poses numerous issues that require careful thought. I fear that by rushing, we could foreclose the opportunity to design a commission we can be confident would be an effective use of taxpayers' dollars. It would be ironic if those arguing for a deliberate, thorough commission review of privacy issues do not give deliberate, thorough consideration to issues relevant to establishing such a commission.

I think it's worthy noting that the pace in which the committee is moving on this proposal to study privacy stands in stark contrast to the complete lack of attention the committee has paid to legislation that would actually establish privacy protections. For example, in May of last year, Mr. Condit, myself, Mr. Markey, Mr. Dingell, Mr. Turner, and many other colleagues on this committee and others introduced legislation that would establish comprehensive privacy protections for individuals' medical records. That bill was referred to this very subcommittee, yet 12 months later there's been no consideration whatsoever of that bill or other medical privacy proposals that have been referred to this subcommittee.

As we examine the merits of H.R. 4049, it's imperative that we remember that Congress has a responsibility to do more than request the study of privacy issues. Congress should act immediately to address serious privacy concerns in several areas. For example, many individuals currently are withholding medical information from their health care providers, even avoiding medical care for fear of privacy violations.

Years of congressional hearings and study by governmental and nongovernmental entities have provided us with more than sufficient information to take action to enact comprehensive medical privacy protections. Congress also must ensure that adequate privacy protections apply to individuals' financial information.

One of the questions that has arisen about the Privacy Commission proposal is whether a commission would delay ongoing privacy initiatives. I understand the proponents of the legislation have emphasized that this measure is intended to complement, not delay, ongoing efforts. However, I think that an April 17, 2000, editorial in the Life and Financial Services edition of the National Underwriter magazine provides insight into this issue. The editorial chides the Financial Services Coordinating Council, which represents insurance companies and securities firms, for failing to endorse H.R. 4049, arguing that, "by not lending its considerable weight to the effort to enact the bill, FSCC may be missing a golden opportunity to forestall highly restrictive privacy measures that will be introduced both in Congress and in State legislatures around the country."

The editorial further stated, "If the financial services industry can make a strong economic case for the consumer benefits of information-sharing, the bipartisan Commission proposed by Representatives Hutchison and Moran provides the best forum to do it. Moreover, the presence of such a commission will provide a strong argument for Congress and the State legislators to wait for the results before enacting highly restrictive privacy legislation."

This editorial underscores that despite the best intentions of the proposal's authors, others may well want to use it to impede privacy protection efforts.

If we are to move forward with H.R. 4049, we must ensure that any privacy commission created is structured so that its deliberations will involve consensus-building instead of divisiveness, and so that members on the Commission have appropriate expertise and experience. Further, the Commission's resources and powers must be consistent with the mandate it is expected to carry out.

In this week's hearing on the bill, we are receiving testimony from individuals who have been involved with the study of privacy or who have worked on privacy initiatives. These witnesses can help us better understand the issues relevant to constructing an effective commission. I look forward to the testimony of today's witnesses.

I want to note that in addition to statements submitted yesterday for the record, I've received comments on this bill from privacy consultant Robert Gelman and would like to enter his statement into the record. I also request that we keep the record open for 2 weeks.

Mr. HORN. Without objection, that will be put in the record.

[The prepared statement of Hon. Henry A. Waxman follows:]

STATEMENT OF REP. HENRY A. WAXMAN
LEGISLATIVE HEARING ON H.R. 4049
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
May 16, 2000

Mr. Chairman, I want to commend you for holding hearings today and yesterday on H.R. 4049. I regret that I was unable to attend yesterday's session due to a pre-existing schedule conflict, but I understand that the session was informative.

H.R. 4049 proposes a $2.5 million privacy commission to study a wide range of very complex issues that affect a tremendous number of stakeholders. It is important to examine this proposal carefully and ensure that those with relevant expertise and experience have had a chance to review it, and I appreciate that you facilitated that process with this week's hearings.

The schedule the Subcommittee has set for moving this legislation forward, however, may be self-defeating. Many of us want strong privacy bills, but the rushed pace we are following with this bill may result in legislation that is counterproductive to privacy efforts.

H.R. 4049 was introduced at the end of March. The Subcommittee announced last week that the Subcommittee is interested in having a markup by next week. This intention to mark up this bill by next week was announced before the Subcommittee even heard from the many experts that are coming before

Subcommittee this week -- and, as we saw from testimony and statements provided yesterday, the bill poses numerous issues that require careful thought. I fear that by rushing we could foreclose the opportunity to design a commission we can be confident would be an effective use of taxpayer dollars. It would be ironic if those arguing for a deliberate, thorough commission review of privacy issues do not give deliberate, thorough consideration to issues relevant to establishing such a commission.

I think it is worth noting that the pace at which this Committee is moving on this proposal to study privacy stands in stark contrast to the complete lack of attention the Committee has paid to legislation that would actually establish privacy protections. For example, in May of last year, Mr. Condit, myself, Mr. Markey, Mr. Dingell, Mr. Turner, many other colleagues on this Committee, and others introduced legislation that would establish comprehensive privacy protections for individuals' medical records. That bill was referred to this very Subcommittee. Yet, 12 months later, there has been no consideration whatsoever of that bill or other medical privacy proposals that have been referred to this Subcommittee.

As we examine the merits of H.R. 4049, it is imperative that we remember that Congress has the responsibility to do more than request the study of privacy issues. Congress should act immediately to address serious privacy concerns in several areas. For example, many individuals currently are withholding medical information from their health care providers, even avoiding medical care, for fear of privacy violations. Years of congressional hearings and study by governmental

and nongovernmental entities have provided us with more than sufficient information to take action to enact comprehensive medical privacy protections. Congress also must ensure that adequate privacy protections apply to individuals' financial information.

One of the questions that has arisen about the Privacy Commission proposal is whether a commission would delay ongoing privacy initiatives. I understand that proponents of the legislation have emphasized that this measure is intended to complement, not delay, ongoing efforts. However, I think that an April 17, 2000, editorial in the "Life and Financial Services" edition of the *National Underwriter* magazine provides insight into this issue. The editorial chides the Financial Services Coordinating Council (FSCC), which represents insurance companies and securities firms, for failing to endorse H.R. 4049, arguing that:

> "by not lending its considerable weight to the effort to enact the bill, FSCC may be missing a golden opportunity to forestall highly restrictive privacy measures that will be introduced both in Congress and in state legislature around the country."

The editorial further stated:

> "If the financial services industry can make a strong economic case for the consumer benefits of information sharing, the bipartisan commission proposed by Reps. Hutchinson and Moran provides the best forum to do it. Moreover, the presence of such a commission will provide a strong

> argument for Congress and the state legislatures to wait for the results before enacting highly restrictive privacy legislation."

This editorial underscores that, despite the best intentions of the proposal's authors, others may well want to use it to impede privacy protection efforts.

If we are to move forward with H.R. 4049, we must ensure that any privacy commission created is structured so that its deliberations will involve consensus building instead of divisiveness, and so that members on the commission have appropriate expertise and experience. Further, the commission's resources and powers must be consistent with the mandate it is expected to carry out.

In this week's hearings on the bill, we are receiving testimony from individuals who have been involved with the study of privacy or have worked on privacy initiatives. These witnesses can help us better understand that issues relevant to constructing an effective commission. I look forward to the testimony of today's witnesses. I want to note that, in addition to statements submitted yesterday for the record, I have received comments on this bill from privacy consultant Robert Gellman, and would like to enter his statement into the record. I also request that we keep the record open for two weeks so that others with expertise and interest in these issues may also submit their comments.

ROBERT GELLMAN
Privacy and Information Policy Consultant
431 Fifth Street SE
Washington, DC 20003

202-543-7923
Fax: 202-547-8287
rgellman@cais.com

May 12, 2000

The Honorable Henry Waxman
House Committee on Government Reform
B-350A Rayburn HOB
Washington, DC 20515

Dear Mr. Waxman:

This letter responds to a request from your staff for comments on H.R. 4049, a bill to establish the Commission for the Comprehensive Study of Privacy Protection.

Information about my background may help to evaluate my comments. I worked on the staff of the House Subcommittee on Government Information from 1977 through 1994. I was the principal staffer responsible for privacy during that period. The first hearing I ever organized was to receive the report of the Privacy Protection Study Commission in 1977. I also worked on legislation designed to establish a permanent privacy commission. I am familiar with the operation of privacy agencies around the world.

I believe that the United States needs a permanent privacy policy agency rather than another temporary study commission. Most other western industrialized countries have privacy agencies, and these agencies have proved to be effective in representing privacy interests and assisting with the implementation of privacy laws. U.S. privacy laws and activities are more cumbersome, more expensive, and less effective because of the lack of a privacy agency. Just about every privacy study conducted in the last couple of decades has recommended establishing a permanent federal privacy agency. For a review of some past studies and recommendations, see my 1993 article *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199 (1993).

Dealing with privacy is a continuous process today and not a one-time event. We spend too much time reinventing the wheel every time a privacy issue arises concerning public records, health records, bank records, marketing records, etc. Privacy needs permanent representation in an independent agency that has no other responsibilities.

The Federal Trade Commission does some privacy work, but it shows interest in privacy only when the subject is in the headlines. The FTC has disappeared from the privacy landscape for years at a time in the past. The FTC should retain its enforcement responsibilities for privacy, but policy leadership belongs elsewhere.

I do not recommend that a privacy agency have regulatory powers. I believe that much progress could be made if a privacy agency were given the task of seeking the general

implementation of Fair Information Practices by government and business record keepers. The agency should be organized in the same way as independent regulatory commissions, but without regulatory powers. A privacy agency could also undertake educational, investigatory, and research activities.

Having stated what I favor, let me explain some of my specific concerns about H.R. 4049.

1. **The Commission's charge is too broad and too unfocused.** Under the bill, the Commission's general goals include identifying privacy threats, analyzing information sharing, reviewing and making recommendations on legislation, regulations, and self-regulatory efforts, and analyzing privacy costs. Subjects include the Privacy Act of 1974 and the Freedom of Information Act, pending congressional legislation, and governmental and private sector privacy protection efforts. The bill also mentions medical, financial, insurance, drivers, and education records, Social Security numbers, and the Internet. This is too much work to be accomplished in 18 months. Just reviewing the Privacy Act of 1974, a law that is outdated and badly in need of a total revision, would take 18 months. If a Commission is to be established, it must be given a specific set of well-defined tasks.

2. **The Commission is required to hold too many hearings**. Holding hearings as a way of gathering facts and opinions is appropriate, but the bill's schedule of 20 hearings to be held in five geographical regions is excessive. Travel costs for 17 members plus staff together with other hearing expenses would soak up most of the Commission's budget.

3. **It is not clear that a Commission will resolve any existing differences on privacy.** Privacy has become a major issue in the last few years, and many companies and organizations have well-entrenched positions. It is unlikely that a high-profile commission, politically appointed and consisting of representatives of these institutions, will accomplish much. The recently completed Internet tax commission offers an example of a study that resulted in nothing useful because the politics of the issue prevented any consensus. The Privacy Protection Study Commission in 1977 operated in a somewhat less politically charged environment, and it did manage a consensus. But few of its recommendations were seriously considered by the Congress and very few were adopted. In retrospect, the Privacy Protection Study Commission was largely a failure even though it began its life under more favorable circumstances than the proposed new Commission will.

Indeed, in some areas, the issues and alternatives are already well-known. For example, consider health privacy. Legislation has been pending before the Congress for years, but there is not enough consensus for action. The issues have been studied and analyzed, and serious attempts to find compromises have been attempted in the House and the Senate. We have already had several major independent studies of health privacy, complete with horror stories and recommendations. It is hard to see how a new Commission will contribute anything useful on health privacy.

In other areas, it would be useful to find facts about the flow of personal information between companies, across the Internet, and among government agencies. However, we do not need a high-level politically appointed Commission to find facts.

Other areas also need attention. The Privacy Act of 1974 is a good example of a law that needs a major overhaul, but no existing institution has the time, resources, or interest to do the work. The Act applies only to the federal government, and it is not clear that a politically appointed Commission is needed to recommend changes. Indeed, appointed Commissioners would find the task of recommending changes to the Privacy Act to be boring.

4. **Useful alternatives to a Commission should be considered.** The political and cost problems associated with a Commission can be avoided by asking a neutral, technically skilled organization to study specific privacy issues. For example, the Computer Science and Telecommunications Board (CTSB) at the National Research Council has policy and information technology expertise. Its work deals with computers, telecommunications, and their application in the real world. Those are the relevant skills for addressing many privacy issues and for considering the consequences of ever-changing technologies with implications for privacy. The CTSB would be useful in reviewing the Privacy Act of 1974 and making recommendations for updating the law to reflect the use of computers and the Internet by the federal government. The CTSB could also tackle other privacy issues, especially those relating to the Internet.

5. **The legislation has technical problems that will interfere with the Commission's work.** First, the Commission does not have enough money to fulfill its mission.

Second, the director is appointed by the Commission and not by the Chairman. That means that no work can be started until the Commission's first meeting. That is bad enough, but any disagreement over the director could delay work for an extended period.

Third, the Commission needs more than one senior staff member. I recommend that the bill provide for a general counsel as well. It will be hard to attract good people at a GS-15 salary.

Fourth, the Commission should be able to borrow personnel on a non-reimbursable basis from another agency willing to make staff available. Paying for two senior staffers from other agencies would practically bankrupt the Commission.

Fifth, the director appoints the staff on his/her own initiative, without any review or approval by the Chairman or the Commission. I would require approval of the Chair just as a precaution.

Sixth, Members of the Commission serve without pay. The schedule that the bill describes calls for several months of work – at least 20 days of hearings, plus meetings, travel, and writing and reviewing. For appointees supported by companies or trade associations, the money does not matter. However, for some people, especially from the consumer community, the lack of any compensation might well be a barrier to participation. I am concerned that

consumers are likely to be underrepresented on the Commission anyway, and the lack of compensation may create an additional obstacle.

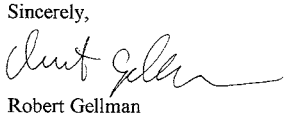
Seventh, the Commission should have the authority to issue subpoenas for testimony and for documents. The Chair should be able to issue a subpoena without a vote of the Commission. The Commission should also be required to protect any personal information that it acquires.

Eighth, the bill should require federal agencies to cooperate with the Commission. A general provision is not enforceable, but the language will be useful nevertheless.

Ninth, the legislation should direct the Commission to select a Vice-Chair. If the Chair gets sick or lazy, a Vice-Chair could step in and provide direction.

I hope that these comments are useful. Please contact me if I can provide any further assistance or answer any questions.

Sincerely,



Robert Gellman

Mr. WAXMAN. My second request is that we keep the record open for 2 weeks so that others with expertise and interest in these issues may also submit their comments.

Mr. HORN. Well, let's try with 1 week, and if there's still some more, because I wouldn't want us to adjourn too much and not get this done. As you say, this is a very important issue, and we've been trying to get a number of people to do something about it. So that's why these hearings. We've got another hearing this week, and everybody is welcome.

Mr. WAXMAN. Mr. Chairman, you're willing to have 1 week for anyone to submit their comments for the record?

Mr. HORN. Yes, and if there's others, we'll work it out. We don't really need a rule on it. We'll just put it all in the record.

[The prepared statements of Hon. Jim Turner and Ms. Blumenthal follow:]

Statement of the Honorable Jim Turner
GMIT Legislative Hearing: H.R. 4049, "To Establish the Commission for Comprehensive Study of Privacy Protection"
May 16, 2000

Thank you, Mr. Chairman. This is the third hearing that we have scheduled on H.R. 4049, and I commend the Chairman for his focus on this issue. Privacy stories have dominated the headlines and nightly news. It is an area of vital importance to the American people and they are understandably demanding that their personal data be protected now. As a result, numerous privacy initiatives at the state and federal level having been moving through the process, and I want to ensure that these are not delayed as a result of this bill. As I have mentioned before, I am pleased to be a cosponsor of this legislation which creates a Commission to study privacy issues, and I commend Congressman Hutchinson and Congressman Moran for their leadership on this bill. However, I want to precede cautiously and ensure that we carefully consider all the implications such a Commission might create.

In light of the concerns that other witnesses have raised, members of past and present entities charged with studying privacy issues have been asked to testify before the Subcommittee. These witnesses are expected to provide their perspective on the types of expertise and background that should be sought in Commission members, the types of issues that should receive focus by the Commission, and the types of reviews that may be redundant. Additionally, we have invited our colleagues, Congressman Barton and Congressman Markey of the Congressional Privacy Caucus, to testify. I also welcome Congressman Greenwood and thank him for his testimony.

Again, I commend the Chairman for holding these hearings and welcome the witnesses here today. Hopefully, as a result of these hearings, we will be moving forward on our goal of providing sound privacy protection for all Americans in a timely fashion.

Written Statement

of

Marjory S. Blumenthal
Director
Computer Science and Telecommunications Board
Commission on Physical Sciences, Mathematics, and Applications
The National Academies

on

The Proposed Commission for the Comprehensive Study of Privacy Protection

Submitted to the
Committee on Government Reform
U.S. House of Representatives

May 15, 2000

Marjory S. Blumenthal
Written Statement
Page one

This statement is intended to provide input into the consideration of the proposed Commission for the Comprehensive Study of Privacy Protection, addressed in H.R. 4049. It draws from my experience as the director of the Computer Science and Telecommunications Board (CSTB) of the National Academies, as well as prior experience in the former U.S. Congress Office of Technology Assessment. The National Academy of Sciences was formed in 1863 by congressional charter to advise the federal government. CSTB, which dates to 1986, is chartered within the National Academies to address the full range of technical and policy issues associated with information technology (see www.cstb.org), and it has conducted several major, influential studies relating to privacy and security (security providing context in terms of vulnerabilities, threats, and attacks on privacy and mechanisms for preventing, detecting, or recovering from same).

The need for thorough consideration of U.S. privacy policy and the risks and opportunities to privacy presented by information technology is self-evident—incidents relating to privacy on the Internet are the stuff of daily news, as well as congressional hearings and federal agency inquiries. At issue is the scope of what would be useful and how to proceed. This statement comments briefly on each.

The scope of study proposed appropriately includes both government (at multiple levels) and private sector activities, which each raise privacy issues separately and in their interrelation. Beyond that, the written description in H.R. 4049 is at such a high level that the coverage of various issues is hard to ascertain (e.g., attention to employer-employee rights and responsibilities, effectiveness as well as potential for self-regulation v. government regulation, evolving technical capabilities that promote or contain privacy risks, procedural options that promote or contain privacy risks and their relation to technical mechanisms, expectations for changes in circumstances over time and the achievement of flexible approaches that are responsive to such changes, and so on). The proposed report contents, for example, call for comment on the "purposes for which sharing of information is appropriate and beneficial to consumers," but the hard problems relate, as they often do, to the details: how much of what kind of information would achieve what benefits, to whom, and at what costs, to whom? What are the choices and tradeoffs?

The complexity of the situation should not be underestimated: as CSTB illustrated in its assessment of the privacy of electronic medical records, *For the Record* (National Academy Press, 1997), the electronic capture and communication of sensitive personal information is expanding from multiple sources, while the set of parties with some interest in or expectation for access to that information is also expanding, and there are

numerous choices that can be made by different classes of individuals, organizations, industries, and government entities at various levels, only some of which may be captured by institutional and/or government policies. CSTB's assessments of cryptography policy and of government systems modernization projects make clear that balancing high-level public and private sector interests can be difficult, let alone conflicting interests within the private sector (or within the public sector, for that matter). Further, the global nature of the economy and increasing numbers of information flows makes it important to view U.S. circumstances from an international perspective, as recent negotiations with the European Union have made clear. Therefore, the remainder of this statement will concentrate on questions relating to how to proceed in studying privacy issues.

A critical element of a study is the selection of the participants. H.R. 4049 focuses on political distribution of participants and their selection without comment on their intellectual and attitudinal qualities. CSTB (and the National Academies generally) use processes aimed at developing study committees with diversity of many kinds, providing a microcosm of the differing relevant perspectives. Elements of these processes, which are labor-intensive, include the following:

- Staff casts a wide net, through conversations with known experts or proponents of differing views and written and oral solicitations of nominations from a wide range of organizations (scholarly, business, professional, nonprofit) and individuals (knowledgeable authorities on the topic), to generate a list of candidates for the committee.

- Committee candidates are organized to provide sets of alternative choices for categories of committee membership that are differentiated by kind of expertise and outlook on the topic. Primary experts are sought, as opposed to designated policy officials of, for example, trade associations. Individuals are nominated as individuals, on the merits of their expertise and potential to contribute to the committee, not as representatives of specific organizations.

- Selection of the sets of candidates by category factors in additional kinds of diversity, including geographic, demographic (sex, race/ethnicity, age), and affiliation (e.g., different kinds of industry, university and other scholarly institution). Affiliation, like public statements and other expressions of opinions on the topic, are characterized as the "biases" of committee members, and effort is made to balance biases, that is, achieve a range of outlook and opinion that will promote balanced consideration of the issues. By contrast, people who are believed to have a conflict of interest, defined as an ability to profit directly, personally, and significantly from the plausible outcome of a study, are excluded from membership.

- The full set of nominated candidates is reviewed at multiple levels within the National Academies and ultimately approved by the president of the National Academy of Sciences, with the review considering the balance and composition of the proposed committee as well as the caliber of specific nominations. Following acceptance of an invitation to serve, the names, affiliations, and brief biographies of the proposed committee are posted on the National Academies Web site for a period of public comment before committee membership is deemed established.

Selection of a committee chairperson involves the same processes, but often occurs early on, so that that individual can assist in the composition of the committee. It is important that the chairperson be perceived as without bias on the topic and broad in outlook and/or knowledge, as well as demonstrably capable of listening and leading.

Another critical element is the nature of the outcome. At the National Academies, we often strive for a consensus report. With a contentious, charged topic, that can be difficult, but even a consensus description of the problem and framing of options can help to advance the debate. It may be inevitable with a congressional commission, as suggested by the recent commission experience relating to taxation of commerce over the Internet, that the political nature of the process hampers achievement of consensus; the language calling for a majority report and inviting dissenting minority report reinforces the likelihood of a failure to achieve consensus and sends a signal that consensus isn't important. If that is true, however, it calls into question the value of a commission as compared to one or more hearings that feature differing points of view, and it also raises questions about how to tailor the scope of inquiry to fit the means. That is, if the means are likely to be politicized, should the scope be narrower to increase the likelihood of a useful outcome?

Consensus in this arena will be difficult. At CSTB we have seen that even in such areas a cryptography policy (*Cryptography's Role in Securing the Information Society*, National Academy Press, 1996) and intellectual property in the Internet environment (*The Digital Dilemma*, National Academy Press, 2000), it is possible to achieve consensus from a mixed, representative group on important points. Doing so is not easy; it takes time for people to be exposed to a wide range of inputs and perspectives, to argue and deliberate, and to work out differences and careful wording. The National Academies process provides a neutral, apolitical meeting ground and experienced professional staff support that foster inquiry, discussion, and agreement. The emphasis on committee deliberation contrasts to the approach of the former Office of Technology Assessment and many think-tanks, which consult with outside experts but rely on staff to formulate the analysis and conclusions. That process is perhaps more efficient to execute, but it is one step removed from the more direct expression of a mixed group.

A comprehensive examination of the technical, economic, social, and legal dimensions of the privacy policy challenge would be valuable. It is high on the list of CSTB's own objectives, because of the compelling need and the value of a neutral, balanced analysis at this time. I am pleased to contribute to the Committee's evaluation of a proposed approach to the problem, and I forward to the outcome of this process and to contributing further to progress in this important area of public policy.

Mr. HORN. The gentleman from Arkansas. Thank you. The other member from the full committee. We're always glad to have you here.

Mr. HUTCHINSON. Thank you, Mr. Chairman. I want to express my appreciation to the ranking member of the full committee, Mr. Waxman, for his thoughtful letter that he sent after the first round of hearings.

As everyone knows, this is the third day of hearings on this particular Privacy Commission proposal, and I think it is good for America. It's certainly good for this Congress to hear from such distinguished experts on the issues of privacy and to learn the history of what we've done from a legislative standpoint on the issues of privacy and what we need to do, and Mr. Waxman's letter certainly provoked 2 more days of hearings, which is exactly what we need, and I think it has been very, very instructive. So I was pleased that the chairman responded to that request from Mr. Waxman by scheduling yesterday's hearings and today's as well.

I did want to respond to a couple of the remarks of the ranking gentleman who mentioned that he was concerned that we would rush to markup on this bill, a commission bill. Of course, we've passed legislation out of the House in terms of—even though it didn't come into law, we passed a commission for studying campaign finance laws. We've had a Medicare commission. So the structures of commissions have been on the table for some time. But I think it is important that we get the broadest range of input as possible, and I would solicit, Mr. Waxman, any suggestions that you have. We've been in contact with your staff, and we would certainly love your ideas on how this legislation can be improved.

But I think there is a concern in terms of the markup. This is May, and this legislative year consists of June and July. We're out August and in September, and then it's gone. And in a puff of smoke we're out of here, and it's going to be very difficult even on a fast track to get legislation through the House and Senate. And for that reason I would hope that we will continue to move forward this proposal as well as other proposals that have a consensus in this body in terms of privacy. And I think it would be regretful if we went home the end of this year and told the American people we did nothing on privacy. So I hope that we can.

I'm glad the agencies are moving forward. Whatever happens in terms of the agencies, whatever happens in terms of other legislation, it's important that we continue to study this in a thoughtful and comprehensive manner. This mission is designed to complement, complement other issues that are out there and not to be exclusive. I just want to assure the ranking member that that is my intent, and I hope everyone in Congress looks at it the same way.

With that I'll be happy to yield and look forward to the testimony of the witnesses.

Mr. HORN. If the witnesses will stand and raise their right hands to affirm the oath.

[Witnesses sworn.]

Mr. HORN. The six witnesses did affirm. The clerk will note that, and we'll proceed with panel one. The first one is Bob Belair, editor, Privacy & American Business. Glad to have you here.

STATEMENTS OF BOB BELAIR, EDITOR, PRIVACY & AMERICAN BUSINESS; MARY CULNAN, PROFESSOR, McDONOUGH SCHOOL OF BUSINESS, GEORGETOWN UNIVERSITY; CHRISTINE VARNEY, FORMER COMMISSIONER, FEDERAL TRADE COMMISSION; SOLVEIG SINGLETON, DIRECTOR OF INFORMATION STUDIES, CATO INSTITUTE; RON PLESSER, LEGISLATIVE COUNSEL, 1977 PRIVACY COMMISSION; AND STANLEY SOKUL, MEMBER, ADVISORY COMMISSION ON ELECTRONIC COMMERCE

Mr. BELAIR. Thank you, Mr. Chairman. Let me commend you and the members of the subcommittee, and Mr. Hutchison and my Congressman Mr. Moran for your leadership on this bill. I'm delighted to be here. I think I can catch you up a bit in terms of time. I appreciate your rescheduling me from yesterday when I couldn't make it to today, and mindful of that and the big panel, I'll be very, very brief.

Let me just say first in response to Mr. Waxman's comments, Privacy & American Business, we are not for delay. We have supported health information privacy legislation. We have supported other types of legislation when we think that that's the right response and when we think it's ready. We will support this legislation and the establishment of a commission in one of our upcoming editorials. We will lay that out. And we'll address our view that this will not lead to delay, as Mr. Hutchison indicated, obviously.

And you folks know better than I do we're at the end of this Congress. It's going to be very, very difficult to get substantive privacy legislation through in this Congress. Obviously it takes time to organize a new Congress, and your bill does provide for interim reports as well, I'm sure, as other kinds of periodic reports to the Congress as necessary. We don't view it as delay. We view it as a very appropriate opportunity to think comprehensively about the privacy issue.

And very briefly let me just say that we support the legislation, and we support the concept of a new privacy commission for three reasons. First of all, the activity with respect to privacy rights now is extraordinary. It is truly unprecedented. One example I think is dramatic. Last cycle, the 1999 cycle for State legislatures, we tracked over 7,000 privacy bills. That's one out of every five bills introduced in the State legislatures. Obviously there's intense regulatory activity at the State level behind that. There's intense activity here. We don't want to slow that down, but on the other hand we think that it's important to take a look at what that legislation is and what it will do, what the consequences and the unintended consequences are.

Second, the underlying developments that are fueling the privacy debate are changing extraordinarily rapidly. The self-regulatory environment changes. The technology environment changes. I think if you would have asked folks in this room 3 years ago to define "cookies," you would have gotten a definition that today we would snicker at and think is very, very naive. The international environment is changing and is uncertain. The business models that have fueled the privacy debate, affiliate sharing, personalization, these, too, are terms that I don't think you would have heard in public debate 3 or 4 years ago. It's critical that we sort this out.

Finally, third, although we've all worked very hard at privacy, and for many of us for a long time, there is an awful lot, in fact, we don't know. The Internet privacy threat is new, and the dimensions of that threat as well as the consequences of regulating the Internet have an enormous number of uncertainties. The public records debate is very important, and what impact on the marketplace and on public safety restrictions on public records could have in the name of privacy is critical.

Obviously we don't yet know what the impact of the Children's On-Line Privacy Protection Act is going to be or the impact of Title V, the privacy provisions in last year's Graham-Leach-Bliley bill. We don't even know—and certainly not in a careful sense—when opt-out and a robust notice makes sense versus when we ought to do opt-in. And if you look at the factors that have been the pivot points for the privacy legislation to date, sometimes it's subject matter such as in financial or medical legislation. Sometimes it's the source, such as legislation that would regulate access to motor vehicle records. Sometimes it's the use that is the key determinant, such as FCRA. Sometimes it's the type of consumer, such as COPPA. Sometimes it's the amalgamation such as the number of bills that would address amalgamating offline and on-line information.

We still have debates about whether the U.S. traditional approach, a sector-by-sector approach, makes sense. We have debates about a privacy regulatory agency, and it's worth noting that while we have been having that debate, the FTC—and I used to be at the FTC, and one of my colleagues, of course, on the panel is a former Commissioner—the FTC has done a lot of good stuff, but the truth is they have emerged as the Nation's privacy regulatory agency. Maybe that's OK, but it's been done without a debate, without consideration.

Preemption remains an issue, and let me just close by saying we really are at a juncture in the road. It's going to change dramatically over the next few years. We need to figure out a way to protect privacy, but also make sure that we use personal information effectively for public safety, to deliver goods and services to consumers for research, to personalize the marketplace, which is going to be such an important economic stimulator so the stakes are high. Let's do it right, and I applaud the subcommittee, and I applaud the sponsors of the legislation and will continue to be supportive. Thank you.

Mr. HORN. Well, I thank you. You did a fine job of summary, and you did it under 6 minutes. So thank you.

[The prepared statement of Mr. Belair follows:]

TESTIMONY OF ROBERT R. BELAIR
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM
MAY 16, 2000

Mr. Chairman and members of the Subcommittee, I am pleased to testify with regard to H.R. 4049, the Privacy Commission Act of 2000. I want to commend Mr. Hutchinson and my Congressman, Mr. Moran, and also commend the Chairman and the members of your Subcommittee for your leadership on this important issue.

I have been an active participant in the privacy debate for approximately 30 years. I have served as Deputy Counsel of the White House Committee on the Right of Privacy in the Ford Administration; as General Counsel of the National Commission on the Confidentiality of Health Records; and as an outside lawyer for the Office of Telecommunications Policy in the Carter White House, as it undertook follow up projects to the recommendations of the original Privacy Protection Study Commission. I'm currently a partner in the firm of Mullenholz, Brimsek & Belair, where I practice privacy law, and, along with Dr. Alan F. Westin, I'm the Editor of *Privacy & American Business*, a privacy publication for the business community.

I am testifying today in support of H.R. 4049. I note with interest that the legislation has been criticized by many in the privacy advocacy community as a proposal for a "Privacy Procrastination Commission". I also note with interest that the commission has been criticized by at least some in the business community out of a concern that the recommendations of such a commission will ultimately encourage the enactment of inappropriate or overbearing privacy legislation.

In fact, the Privacy Commission, with its 18 month timetable coinciding with a new Administration and a new Congress, will not slow us down. Further, I do not think that its recommendations will lead to inappropriate legislation. I do think, however, that the work of the Privacy Commission will lead to better decisions about privacy, both with respect to any legislation and with respect to self-regulatory initiatives. The original Privacy Protection Study Commission, operating in the mid to late 1970s, did a masterful job of sorting out fact from fiction in an expeditious and appropriate way.

I support the legislation (and, by the way, many in the business community also support the legislation) for three compelling reasons.

- First, privacy has become a major, domestic public policy issue. We find privacy stories on the front pages, on the nightly news and even in the movies. Last year, the state legislatures considered over 7,000 privacy bills. Approximately one out of every five bills introduced in the state legislatures was a privacy bill. The Congress currently has before it dozens of privacy bills. The federal regulatory agencies are busy on numerous

privacy initiatives. Simply stated, we are right smack in the middle of a privacy feeding frenzy. The danger, of course, is that legislatures and, even in its wisdom, the Congress (and this applies, as well to various regulatory agencies), will adopt inappropriate, counterproductive legislation. It isn't that we need a cooling off period. What we need is a thinking smart period.

- Second, developments that are relevant to the formulation of privacy policy are moving with unprecedented velocity and extraordinary volatility. Various industries are moving, almost on a daily basis, to embrace increasingly comprehensive and robust, self-regulatory reform. The technology which captures, maintains and disseminates personal information changes almost on a monthly basis. The international situation -- given the EU Data Privacy Directive and the ongoing negotiations on Safe Harbor accords -- continues to involve significant uncertainty. Even the business models that are predicated on the use of personal information -- affiliate sharing and personalization, to name two -- are changing and evolving. Sorting out what is important and what is simply transient background noise or an incidental distraction is a major task in this kind of an environment. A Privacy Commission could serve an important purpose in undertaking this sorting out process.

- Third, despite all of the recent focus on information privacy, the real truth is that there is an enormous amount that we do not know and an enormous amount of work yet to be done.

- From a factual standpoint, for example, we still don't know nearly as much as we need to know about the nature of privacy threats posed in an online environment. We know and appreciate that the public worries about cookies; worries about the capture of information regarding browsing behavior; and worries about profiling. But, we don't know what the dimensions are of the real privacy threats posed by these activities and what the economic payoffs are of these activities. We don't know nearly as much as we need to know about the role that public access to personal information in government-held, public records plays in the marketplace and from a public safety standpoint. Nor do we understand the real dimensions of any privacy threat posed by newly-automated and cumulative public records.

- We certainly don't know very much yet about the impact of recently enacted privacy protection legislation, such as the Children's Online Privacy Protection Act or the privacy protections in Title V of Gramm-Leach-Bliley.

- We still have much to learn about the circumstances under which opt-out is an appropriate privacy protection approach (particularly, when coupled with a clear, conspicuous and robust notice) versus the circumstances in which an opt-in is appropriate. And, of course, we need to identify the circumstances under which normative information is compiled in databases that are used for risk management where no type of choice is appropriate.

- Further, in shaping a privacy policy, there is wide disagreement about the types of factors that should be considered and how much weight each of these factors should be given.

    - Is the subject matter and/or sensitivity of the information the most important factor?

    - Is the source of the information an important factor?

    - What about the intended uses of the information?

    - How much does it matter that the information will be combined with information about the individual from other sources into some type of a profile?

- Similarly, there is wide disagreement about whether the U.S. should retreat from its traditional, sector-by-sector approach to privacy protection and, instead, move toward a European-type, comprehensive or global approach.

- Along the same lines, there is wide disagreement about whether the U.S. should move toward the establishment of some type of national privacy regulatory agency or whether the existing combination of courts, consumer protection authorities, Attorney Generals and various federal agencies provide a more than adequate

privacy regulatory presence. Indeed, there are those who argue that, while this debate has been going on, the FTC has effectively emerged as a *de facto* national privacy protection agency.

- And, what about the vexing question of preemption? In an electronic environment, in an environment where information moves across state borders in nanoseconds, does it really make any sense to allow the location of data, sometimes the momentary location of data, to dictate the rules that apply? Should we not be moving toward national privacy rules instead of a balkanized arrangement in which each state gets to set its own rules, sometimes in ways that can place a thumb to the windpipe of national and interstate commerce?

Finally, it cannot be overemphasized that the stakes are high -- very high -- in finding appropriate and effective answers to these questions and, ultimately, in reshaping our national privacy and information policy. As a nation, we must find a way to protect information privacy and to give our citizens confidence that they can engage in e-commerce and provide access to their personal information, knowing that the information will be used appropriately and in ways that comport with their understanding of the transaction or event.

At the same time, we must preserve the ability of the business community (and, for that matter, of the government) to use personal information effectively for vital risk management determinations; for medical and other kinds of research; to promote consumer convenience and to drive down the cost and improve the quality of goods and services; and to personalize the

marketplace -- in a very real sense, revolutionize the marketplace -- to spur growth and to give consumers information about the goods and services which consumers wish to receive.

The Privacy Commission created by H.R. 4049 will not answer every question to everyone's satisfaction. But, there is every reason to believe that this is exactly the right time for a Privacy Commission to look at these questions, as well as the profound changes in the underlying technology and the underlying business models that have ignited the current privacy debate. I do not believe that this will slow us down. I do believe, however, that this will allow us to get to our destination with fewer mistakes and in a way that encourages the effective use of personal information while protecting privacy.

Thank you.

Mr. HORN. Dr. Culnan.

Ms. CULNAN. Thank you, Chairman Horn. Thank you for inviting me to testify. I also want to thank Representative Waxman for his interest in support of this issue, and to Representative Hutchison for introducing the legislation.

My name is Mary Culnan, and I'm a professor at Georgetown University, where I teach electronic commerce. I also bring additional background to this panel as I have served as a Commissioner on the President's Commission on Critical Infrastructure Protection, and I also finished just this week serving as a member of the FTC Advisory Committee on Access and Security.

I also support the establishment of a privacy commission. Bob Belair did an excellent job of summarizing some of the issues that commend the establishment of such a commission. I don't think anyone could have foreseen in 1977 the changes that the personal computer and the Internet would bring in our work lives, our home lives and in the world in general today. So I think it's time to revisit these issues on a broad, comprehensive scale, because most of our legislative efforts have been sectoral.

I only want to address two primary concerns I do have about the legislation, and I raise some other issues in my written testimony. The first issue is that H.R. 4049 doesn't specify any criteria for the Commission to use in performing its evaluation, and I think this is a major shortcoming. Since the PPSC issued its report in 1977, fair information practices have emerged as a global standard for striking an appropriate balance between protecting individual privacy and allowing appropriate uses of information for a lot of the purposes that Bob Belair described.

There is not consensus on how to implement fair information practices, but there is a consensus that they are global standards, and I believe the Commission's findings and recommendations should be based on the extent to which fair information practices have been implemented across the domains of the Commission's work. They should also be used as criteria to evaluate the current efforts that have been undertaken to protect privacy that are specified in the legislation both in the private sector, the Federal Government, and in the States.

My second concern is that of a taxpayer, since I will be helping to fund the Commission. I think the legislation defines an ambitious agenda for the Commission. I have some concerns that the Commission will be able to complete its work in the time specified, given that it's required to hold so many hearings. I believe the number is 20. While public hearings are an important way to gather information and to make the Commission's work accessible to the public, many privacy issues are complex, and public hearings are not necessarily the most effective forum to sort these issues out in detail. When I served on the PCCIP, we held one half-day public hearing in each of five regions of the country. We also had meetings with business executives, academics, and government officials in each city. We held a number of conferences and workshops, and we were briefed by a wide range of individuals and organizations. Overall we had contacts with more than 6,000 associations, corporations, government agencies, and individuals.

I think the Commission will need to use a variety of methods, including public hearings, for gathering information. Since the commissioners are going to be serving without pay, the legislation will need to better balance the time demands of serving on the Commission with the demands of the Commissioners' existing job responsibilities. They will be able to do much of their work electronically, but they will also need to meet in person to take testimony, for briefings and to deliberate. There should be at least one hearing in each region of the country, but given there is probably an upper limit on the amount of time people can devote, I think the Commission should decide what methods will best help make its members able to complete their work.

And then finally I would like to second Representative Waxman's call about appointing people to the Commission who can work together and promote a consensus, because these issues are very difficult. It's very important that the Commission represent a range of expertise and perspectives. Otherwise its results will not be credible. But if the people—if it's a very fractious group, also they won't be able to work together to promote a consensus, and I think that's awfully important.

So I want to thank you again for inviting me to testify, and I look forward to your questions.

Mr. HORN. Thank you very much. You did it all within 5 minutes. So thank you. I didn't know professors could speak in less than 50-minute modules. Since I am a professor, I have great difficulty with this committee. Thank you very much.

[The prepared statement of Ms. Culnan follows:]

PREPARED STATEMENT OF DR. MARY J. CULNAN

Professor, The McDonough School of Business
Georgetown University
Washington, D.C.

Legislative Hearing on H.R. 4049
Bill to Establish the Commission for the Comprehensive Study of Privacy Protection

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

Washington, D.C.
Tuesday, May 16, 2000

Chairman Horn and members of the Subcommittee, thank you for inviting me to testify. My name is Mary Culnan. I am a professor at the McDonough School of Business, Georgetown University where I teach electronic commerce. I have been conducting research on the impact of technology on consumer privacy for more than a decade. I am also the author of the 1999 Georgetown Internet Privacy Policy Survey. In 1997, I served as a Commissioner on the President's Commission on Critical Infrastructure Protection (PCCIP)[1] and I have just finished serving as a member of the Federal Trade Commission's Advisory Committee on Access and Security. This is the eighth time I have testified before Congress on information privacy issues.

I support the creation of the Commission for the Comprehensive Study of Privacy Protection. It has been more than two decades since the Privacy Protection Study Commission (PPSC) issued its landmark report in 1977. Since then, the personal computer and the Internet have transformed our economy and the way we work and live. At the same time, these advances in information technology that provide benefits to both organizations and individuals simultaneously raise new privacy issues that the 1977 study could not have envisioned. Because the economy now moves on Internet time, technology is often ahead of social norms. For example, because today the same hardware and software platforms are used by so many individuals and organizations, new features or "Code" that can be developed by a single individual or firm have the potential for widespread social impacts. These features can either threaten important social values such as privacy, or they can be used create self-regulatory solutions that promote important social values. It is time to revisit the issues from the 1977 report as well as the new issues raised by the information economy on a broad scale and the Commission creates an opportunity to do just that. However, I do have some concerns about some of the specifics of the pending legislation, H.R. 4049, which I will address here.

My testimony will address two main topics. I will begin by discussing some issues related to the scope of proposed Commission's work. Second, I would like to

[1] The President's Commission on Critical Infrastructure was created by President Clinton by Executive Order 13010 of July 15, 1996. The PCCIP was tasked to develop policy recommendations for protecting and assuring eight critical national infrastructures including the Internet. President Clinton issued PDD 63 on May 22, 1998 which called for implementation of the Commission's recommendations. See www.ciao.gov.

address issues related to the operations of the Commission, drawing on my experience as a Commissioner on the PCCIP.

Comments on the Scope of the Commission's Work

H.R. 4049 calls for the Commission to undertake a broad assessment of the privacy issues we are facing today and includes both the private sector as well as the federal, state and local governments. The Commission needs to look ahead in its research and its findings as it may be difficult to assess the future by looking in the rear view mirror. For example, the emergence of the Internet as a critical infrastructure raises new issues related to the appropriate balance between individual civil liberties and our national security interests. Individuals are beginning to move their personal information from the personal computers in their homes that enjoy certain Fourth Amendment protections, to Web databases that do not enjoy the same protections. Today we are on the doorstep of yet another revolution based on wireless technology that promises to raise an entirely new set of privacy issues we have not begun to contemplate. While the Commission's responsibilities are specified broadly, its usefulness will be short-lived if it only focuses on today's technologies and privacy issues and fails to address these emerging issues.

Second, a major shortcoming of H.R. 4049 is that it does not specify any criteria for the Commission to use in performing its evaluation. The PPSC's conclusions were based on three concurrent policy objectives: minimize intrusiveness, maximize fairness and to create legitimate, enforceable expectations of confidentiality.[2] In the more than two decades since the PPSC issued its report, fair information practices have emerged as the global standard for striking an appropriate balance between protecting individual privacy and allowing appropriate uses of information. At the heart of fair information practices are the following principles:

- Notice about what personal information is collected and how it will be used,
- Choice (e.g. opt out) about subsequent uses of personal information for other unrelated purposes,
- Access to personal information and the ability to correct any errors,

- Data Stewardship including integrity and security for data during transmission and storage, and
- Enforcement and redress to ensure that organizations adhere to their stated policies and that they provide consumers and citizens a with method for resolving privacy concerns.

Fair information practices serve as the basis for U.S. privacy laws (e.g. Privacy Act of 1974) and self-regulatory programs (e.g. TRUSTe and BBBOnline privacy seals) as well as international privacy laws (e.g. EU Privacy Directive). While there is widespread consensus about fair information practices as general principles, consensus does not currently exist about how the principles should be applied in practice across sectors.[3]

H.R. 4049 contains no mention of fair information practices. The Commission's findings and recommendations should include an assessment of the extent to which fair information practices have been implemented across the various domains of the Commission's work. Fair information practices should be used to evaluate current efforts to address privacy issues by Federal and State governments, individuals or entities (Section 4(a) (2)) and in the sections of the Commission's report where the effectiveness of current efforts to protect privacy are assessed (Section 4(c)(2)(C)). Where fair information practices are found to be lacking, they can serve as a basis for recommending new legislative or non-legislative options (Section 4(c)(2)(D and G)[4].

---

[2] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, 1977, p. 15.
[3] See for example the Final Report of the FTC Advisory Committee on Access and Security, May 15, 2000, available at www.ftc.gov/acoas.
[4] For example, the 2000 Web Sweep performed by the FTC found that while the vast majority of popular Web sites posted privacy disclosures, only 20% of these disclosures included all elements of fair information practices. See Glenn R. Simpson, "FTC Finds Web Sites Fail to Guard Privacy," *Wall Street Journal.*" May 11, 2000, p. B12.

Finally, H.R. 4049 is silent on two issues which merit study by the Commission. First, the section of the bill dealing with the study states that the scope includes information activities by the States but does not call for an analysis of current or pending State privacy legislation. Second, there is no mention of workplace privacy issues in the bill. The PPSC assessed workplace privacy issues in the mainframe computer era and it would be appropriate to revisit this issue today given the technology revolution in the office.

Comments on the Operational Aspects of the Commission

H.R. 4049 defines an ambitious agenda for the Commission. I have some concerns about the ability of the Commission to complete its work in eighteen months given the requirement to hold so many public hearings. Public hearings are an important way to gather information and to make the Commission's work accessible to a wide range of stakeholders. However, short public statements do not effectively communicate the nuances of complex technologies or business processes, nor do public hearings lend themselves to the types of important candid discussions that take place in a less public setting with no press in attendance.

At the PCCIP, we held a one half-day public hearing in each of five regions of the country. In each city, the Commissioners also had individual meetings with business executives, academics and government officials for the remaining half-day. We held public meetings in Washington, DC with our Advisory Committee. We also held a number of conferences and workshops, and were briefed by a wide range of individuals and organizations. Overall, we had contacts with approximately 6000 associations, corporations and government agencies.

In my opinion, the workshops were the most productive method of information gathering. These were full-day roundtable discussions that were organized and facilitated by a contractor. Each workshop was devoted to a single topic (e.g. business practices and concerns in a particular industry). The format promoted a full and candid exchange of information and perspectives among the workshop participants and the Commissioners.

I believe that the Commission will need to employ a variety of methods, including public hearings, for gathering information. As the Commissioners serve without pay, the legislation will need to balance the time demands of serving on the Commission with the

demands of the Commissioners' existing job responsibilities. While much of the work of the Commission can be performed electronically, there is probably an upper limit on the amount of time Commissioners can invest in travel to hearings and other meetings. Further, most of the current privacy issues are complex problems without obvious solutions. Developing recommendations to address these issues will require face-to-face discussions. I recommend that H.R. 4049 be amended to require at least one public hearing in each of five regions of the country, but leave the final number to the judgment of the Commission as to what would best help the members complete their work.

A strength of H.R. 4049 is the requirement that all members of the Commission be appointed within thirty days after the date of enactment. This will ensure that the Commission is at full strength from the beginning and hits the ground running. To be effective, it is critical that the Commissioners represent a range of expertise and perspectives. This may turn out to be a challenge given that the Commissioners will be appointed by five different individuals. However, if the membership of the Commission is perceived as favoring a single perspective, this will obviously jeopardize the credibility of its findings and recommendations.

Finally, there appears to be one minor factual error in the Findings section of the bill (Sec. 2(10)). This finding appears to be based on the 1999 Georgetown Internet Privacy Policy Survey of which I am the author[5]. The FTC used my findings to prepare its 1999 report to Congress[6]. The Georgetown study found that 67% (not 87%) of Internet sites in the sample provide some form of privacy notice. Because the 1999 study I conducted and the 1998 study conducted by the FTC were based on entirely different populations of Web sites, it is not correct to say that number of such disclosures increased from 14% in 1998 to 67% in 1999. There is, however, anecdotal evidence to suggest there was progress between 1998 and 1999.

This completes my testimony. I welcome your questions and would be happy to work with the Subcommittee as this issue moves forward.

---

[5] See http://www.msb.edu/faculty/culnanm/gippshome.html

[6] See Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress, available at http://www.ftc.gov/os/1999/9907/privacy99.pdf

Mr. HORN. Now Ms. Varney, former Commissioner in the Federal Trade Commission.

Ms. VARNEY. Thank you, Mr. Chairman, Mr. Hutchison, Mr. Waxman. Thank you very much for inviting me to testify this afternoon on H.R. 4049, the Privacy Commission Act. My name is Christine Varney. I'm currently a partner at Hogan & Hartson, and where I chair the Internet Practice Group, and I have served on the Federal Trade Commission from 1994 through 1997, I believe, and did extensive work on privacy while at the Commission.

With your permission, I have submitted for the record extensive descriptions of fair information and privacy practices that can be used for future reference, but I would like to take a few minutes to discuss the bill.

As you know, privacy is not a new issue. As I think you have heard from other panelists, here in the United States we have a long history of examining the rights of Americans to be free from unwanted and unwarranted intrusions, including the collection, use of personal information about them without their knowledge or consent. What is new, however, is that in the information age, the ease with which information about individuals can be gathered, aggregated, and disseminated is unparalleled. There are virtually no costs or meaningful economic barriers any longer to gathering extensive information about individuals and using it for any purpose whatsoever.

This trend has not gone unnoticed by the American public. In survey after survey, Americans are regularly responding that privacy is their No. 1 concern on the Internet. However, this concern goes beyond the Internet. Although the Internet make it is easy to collect, aggregate and transfer information, privacy concerns don't stop in cyberspace. As you know, there has been concern around the use of personal information and potential for abuse of that information for quite some time. Indeed, Congress has already enacted several laws that deal with or touch upon the use of personal information, including, to name just a few, the Fair Credit Reporting Act, the Children's On-Line Privacy Protection Act, the Financial Services Modernization Act, the Electronic Funds Transfer Act, the Electronic Communications Privacy Act, the Drivers Privacy Protection Act, the Telephone Consumer Protection Act, the Cable Communications Policy Act, the Video Privacy Protection Act, and I could go on.

There are also a myriad of State law protections in place. What is missing, in my view, is a comprehensive and thoughtful review of the old and new laws and their effectiveness in the information age. Therefore, I wholeheartedly support the proposals in H.R. 4049 to create a privacy commission. I think Dr. Culnan has raised some serious concern about how to structure the Commission.

Let me say a few more words about commissions, having been a Federal Trade Commissioner. As we have seen with other commissions, the work and the results of the Commission can be directly attributable to the composition of the Commission itself. Should this Commission be established, I would urge that all of those who have the ability to appoint Commissioners consider the commitment of a potential appointee to reach consensus as opposed to furthering an agenda. The issues are complex, and the solutions must

be equally comprehensive. Those who have sat before you and talked about self-regulation as a failure and legislation as the answer, or self-regulation as a panacea and legislation as repugnant are, in my view, clearly missing the point.

The point in the information age has to be how can American consumers, whether they are consuming medical information and services, financial information and services, or other commercial information, protect themselves and their privacy desires? In some instances there will be technological solutions. In some instances there will be best practices, and in other instances there may be loopholes in existing law that need to be closed or absence of law altogether.

Too often the privacy debate has been polarized between those who wish to prohibit the use of personal information for any and all purposes and those who wish to exploit the use of personal information for any and all purposes. Neither of these postures addresses the increasing concerns of Americans regarding protection of their personal privacy while allowing for its beneficial use. Neither of these positions, frankly, can bring a balanced, economically viable and societally appropriate conclusion to the privacy debate.

Thus I would urge that this Commission be created, but that the goal of the Commission be clearly articulated as suggesting to the Congress a legal framework that balances both the economic benefits of the free flow of information with the rights of individuals to maintain their own preferred zones of privacy through whatever means makes sense in any given situation, be those means technological, legal or otherwise.

What will not advance the protection of privacy in the information age is a deadlocked Commission with a faction opposed to any meaningful use of information and a faction opposed to any meaningful limits on the use of information.

Thank you very much.

Mr. HORN. We thank you. That's a very helpful statement, and you're well within time.

[The prepared statement of Ms. Varney follows:]

BEFORE THE

HOUSE SUBCOMMITTEE ON

GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE GOVERNMENT REFORM COMMITTEE

LEGISLATIVE HEARING TO ESTABLISH THE

COMMISSION FOR THE COMPREHENSIVE STUDY OF

PRIVACY PROTECTION

MAY 16, 2000

TESTIMONY OF MS. CHRISTINE VARNEY

ON BEHALF OF

THE ONLINE PRIVACY ALLIANCE

Statement by Ms. Christine Varney
May 16, 2000

The Internet is poised to become an explosive economic growth opportunity that will redefine global commerce in the information age. That growth cannot and will not occur without consumer confidence. Privacy is one of the cornerstones of consumer confidence in the Internet.

Numerous companies and associations have come together to create policies and practices that can make privacy a reality for everyone on the Internet. These companies and associations, the Online Privacy Alliance, are pleased to submit the attached documents. First is the Mission Statement describing the goals of the Online Privacy Alliance, second are the Guidelines for Privacy Policies that are adopted by all Online Privacy Alliance members, third are the Principles for Children's Online Activities, and fourth are the Guidelines for Effective Enforcement of Self-Regulation.

The Online Privacy Alliance has worked diligently to come up with policies that can be applied across many industry sectors. These guidelines, principles and statements reflect not only a deep commitment to online privacy, but also new policies which the Online Privacy Alliance members support. The Online Privacy Alliance believes that when there is use or distribution of individually identifiable information for purposes unrelated to that for which it was collected, individuals should be given the opportunity to opt out of such unrelated use or distribution. Also, the Online Privacy Alliance members believe that self-regulation requires robust enforcement and they are committed to ensuring such.

The OPA and its supporting organizations will continue to work to ensure that effective online privacy practices are adopted and implemented among the private sector. In particular, we will be focusing on continuing outreach through business and consumer education, while increasing awareness of various privacy assurance programs. It has been a pleasure working with this group and I look forward to continuing to work with the Online Privacy Alliance to build consumer confidence in the Internet.

Table of Contents

1. **Online Privacy Alliance Materials**

   - OPA Mission Statement and Membership Pledge
   - Guidelines for Online Privacy Policies
   - Principles for Children's Online Activities
   - Effective Enforcement of Self-Regulation
   - Online Privacy Alliance Association Policy

2. **Privacy Initiatives by Private Sector: A partial review of steps which OPA Supporters have done to help foster consumer confidence by protecting personal privacy in cyberspace.**

3. **A Quick Guide to Helpful Tips and Technical Tools for safeguarding your privacy online.**

4. **The OPA White Paper details a "layered" approach to privacy protection. The paper describes how the enforcement of existing laws by government, combined with industry self-regulation, creates "adequate" safeguards for the protection of personal information collected online in the United States.**

5. **The OPA Commentary document gives background on the development of the OPA Guidelines.**

online privacy alliance

An alliance of global companies & associations committed to promoting privacy online.

Committed Organizations, May 16, 2000

Companies

3Com
Acxiom
AdForce
Advertising.com
America Online, Inc.
Ameritech
Apple Computer
AT&T
Avenue A, Inc.
Bank of America
Bell Atlantic
Bell South
BioNetrix Systems Corp.
Cisco
ClickAgents.com
CommTouch Software
Compaq
Dell
Disney
Dun & Bradstreet
DoubleClick Inc.
eBay Inc.
Eastman Kodak, Co.
EDS
EDventure Holdings, Inc.
E-LOAN
Engage Technologies Inc.
Enonymous Corporation
Equifax
Ernst and Young
Excite@Home
Experian
Ford
Gateway
Geotrust, Inc.
IBM
INFOSISTANT, INC.
InsWeb Corporation
INSUREtrust.com LLC
Intel Corp.
Intuit
KPMG
LEXIS-NEXIS
Lifescape LLC
MCI WorldCom
Microsoft
MindSpring Enterprises, Inc.
MoneyForMail.com
National Foundation for Consumer Credit
NCR
Nestle' USA
NORTEL
Novell
northpole.com. LLC
Preview Travel
PricewaterhouseCoopers
Privada, Inc.
PrivacyRight, Inc.
PrivaSeek, Inc.
Procter & Gamble
RealNames Corp.
Real Networks, Inc
Sagent Technologies
Sun Microsystems
Time Warner Inc.
Unilever United States, Inc.
USinternetworking Inc.
Viacom
ViewCall Canada, Inc.
WebConnect
Wine.com
Women.com Networks
Xerox
Yahoo!

Associations

American Advertising Federation
American Electronics Association
American Institute of Certified Public Accountants
Association for Competitive Technology
Association of Online Professionals
Business Software Alliance
CASIE (CASIE is representing Association of National Advertisers & American Association of Advertising Agencies)
Computer Systems Policy Project (CSPP)
Council of Growing Companies
Direct Marketing Association
Electronic Retailing Association
European-American Business Council
Individual Reference Services Group
Information Technology Association of America
Information Technology Industry Council
Interactive Digital Software Association
Interactive Travel Services Association (ITSA)
Internet Advertising Bureau/FAST
Internet Alliance
Motion Picture Association of America
Software & Information Industry Association
The United States Chamber of Commerce
The United States Council for International Business

online privacy alliance

An alliance of global companies & associations
committed to promoting privacy online.

Mission Statement

The Online Privacy Alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce.

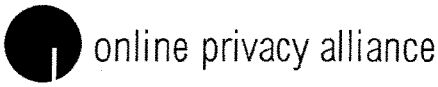
The Alliance will:

- identify and advance effective online privacy policies across the private sector;
- support and foster the development and use of self-regulatory enforcement mechanisms and activities, as well as user empowerment technology tools, designed to protect individuals' privacy;
- support compliance with and strong enforcement of applicable laws and regulations;
- support and foster the development and use of practices and policies that protect the privacy of children;
- promote broad awareness of and participation in Alliance initiatives by businesses, non-profits, policy makers and consumers; and
- seek input and support for Alliance initiatives from consumer, business, academic, advocacy and other organizations that share its commitment to privacy protection.

Membership Pledge

As members of the Alliance:

- we endorse its mission;
- we commit ourselves to implement online privacy policies consistent with the Alliance's guidelines; and
- we commit ourselves to participate in effective and appropriate self-regulatory enforcement activities and mechanisms.



An alliance of global companies & associations
committed to promoting privacy online.

Guidelines for Online Privacy Policies

Upon joining the Online Privacy Alliance, each member organization agrees that its policies for protecting individually identifiable information in an online or electronic commerce environment will address at least the following elements, with customization and enhancement as appropriate to its own business or industry sector.

Adoption and Implementation of a Privacy Policy

An organization engaged in online activities or electronic commerce has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. Organizations should also take steps that foster the adoption and implementation of effective online privacy policies by the organizations with which they interact; e.g., by sharing best practices with business partners.

Notice and Disclosure

An organization's privacy policy must be easy to find, read and understand. The policy must be available prior to or at the time that individually identifiable information is collected or requested.

The policy must state clearly: what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access.

The policy should disclose the consequences, if any, of an individual's refusal to provide information. The policy should also include a clear statement of what accountability mechanism the organization uses, including how to contact the organization.

Choice/Consent

Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use. Additionally, in the vast majority of circumstances, where there is third party distribution of individually identifiable information, collected online from the individual, unrelated to the purpose for which it was collected, the individual should be given the opportunity to opt out.

Consent for such use or third party distribution may also be obtained through technological tools or opt-in.

Data Security

Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. They should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.

Data Quality and Access

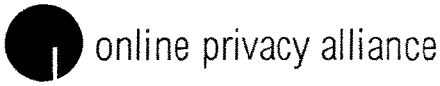
Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used.

Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate consumer access and correction, and protections against accidental or unauthorized alteration.

•••

These guidelines are not intended to apply to proprietary, publicly available or public record information, nor to supersede obligations imposed by statute, regulation or legal process.

Other valuable resources available to Alliance members in the development of privacy policies include: the OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"; the U.S. Department of Commerce's "Staff Discussion Paper of Privacy Self-Regulation"; and various industry association programs.



An alliance of global companies & associations
committed to promoting privacy online.

Principles for Children's Online Activities

The Members of the Online Privacy Alliance believe that the development of interactive online communications provides tremendous opportunities for children. At the same time, it presents unique challenges for protecting the privacy of young children. Children under 13 are special. Unlike adults, they may not be fully capable of understanding the consequences of giving out personal information online. However, children often understand how to navigate online far better than their parents do. Parents will not always have the knowledge, the ability or the opportunity to intervene in their children's choices about giving out personal information. Therefore, companies operating online must protect the privacy of children.

In connection with online activities of children under 13, the Alliance adopts the following principles.

Companies doing business online that operate sites that are directed at children under 13 or at which the age of visitors is known, must at those sites:

- Not collect online contact information from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of this information, which shall include an opportunity for the parent to prevent use of the information and participation in the activity. This online contact information shall only be used to directly respond to the child's request and shall not be used to recontact the child for other purposes without prior parental consent.

- Not collect individually identifiable offline contact information from children under 13 without prior parental consent.

- Not distribute to third parties any individually identifiable information collected from a child under 13 without prior parental consent.

- Not give the ability to children under 13 to publicly post or otherwise distribute individually identifiable contact information without prior parental consent. Sites directed to children under 13 must take best efforts to prohibit a child from posting contact information.

- Not entice a child under 13 by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in that activity.

online privacy alliance

An alliance of global companies & associations
committed to promoting privacy online.

Effective Enforcement of Self-Regulation

Summary

Effective enforcement of online privacy policies is intended to assure an organization's compliance with its privacy policies for the collection, use and disclosure of personally identifiable information online and provide for consumer complaint resolution. Whether administered by a third-party privacy seal program, licensing program or a membership association, the effective enforcement of self-regulation requires: 1) verification and monitoring, 2) complaint resolution and 3) education and outreach. The Online Privacy Alliance believes the best way to create public trust is for organizations to alert consumers and other individuals to the organization's practices and procedures through participation in a program that has an easy to recognize symbol or seal.

Third-Party Enforcement Programs

Validation by an independent trusted third party that organizations are engaged in meaningful self-regulation of online privacy, may be necessary to grow consumer confidence. Such validation should be easily recognized by consumers, for example through the use of a seal or other symbol. The symbol or seal can be used to connote both compliance with privacy policies and an easy method for consumers to contact the seal provider. Thus, the Online Privacy Alliance supports third-party enforcement programs that award an identifiable symbol to signify to consumers that the owner or operator of a Web site, online service or other online area has adopted a privacy policy that includes the elements articulated by the Online Privacy Alliance, has put in place procedures to ensure compliance with those policies, and offers consumer complaint resolution.

Privacy Seal Program

Such a privacy seal program (hereinafter "the seal program") should implement mechanisms necessary to maintain objectivity and build legitimacy with consumers. The seal program should utilize a governing structure that solicits and considers input from the business community, consumer/advocacy organizations and academics in formulating its policies. The seal program should strive to create a consistent and predictable framework in implementing its procedures. The seal program should be independent and should endeavor to make receipt of the seal affordable for and available to all online businesses.

A seal program should include the following characteristics:

- Ubiquity: In order to minimize confusion and increase consumer confidence, efforts shall be taken to ensure ubiquitous adoption, and recognition of seals

through branding efforts, including, for example, co-branding with corporations or associations.

- Comprehensiveness: A seal program should be flexible enough to address issues related to both sensitive and non-sensitive information.
- Accessibility: A seal should be easy for the user to locate, use and comprehend.
- Affordability: The cost and structure of a seal should encourage broad use and should not be prohibitive to small businesses. The cost of a seal will vary based on a number of factors, including the extent and complexity of review, size of the business, the amount and type of individually identifiable information collected, used and distributed, and other criteria.
- Integrity: A seal provider should be able to pursue all necessary avenues to maintain the integrity of the seal, including trademark enforcement actions.
- Depth: A seal provider should have the ability to handle the number and breadth of consumer inquiries and complaints about the potential violation of online privacy policies and should have an established set of mechanisms to address those inquiries and complaints.

Verification and Monitoring

A seal program must require that its participants adopt a privacy policy that comports with the principles endorsed by the Online Privacy Alliance. The scope of this requirement only applies to the participating organization and does not apply to the Web pages of affiliates or other Web pages linked to or from the participating organization's Web page. While these baseline principles should be standardized, individual policies accepted by the seal provider should allow for sector-specific variations. The seal program must then require that an organization put in place either self-assessment or accept the seal program's compliance review prior to awarding the seal.

If a self-assessment system is chosen, it must be pursuant to a rigorous, uniform, clearly articulated and publicly disclosed seal program methodology under which an organization would be asked to verify that its published privacy policy is accurate, comprehensive, prominently displayed, completely implemented and accessible; and that consumers are informed of the consumer complaint resolution mechanisms through which complaints are handled. A statement verifying the self-assessment should be signed by a corporate officer or some other authorized representative of the company. The self-assessment should then be reviewed by the seal program to assure compliance with the methodology. Specific criteria for when a company should improve the implementation of its self-assessment system, adopt further measures, or circumstances when a third-party review is required, should be part of the seal program's methodology for acceptable self-assessment.

Periodic reviews should be required by the seal program to ensure that those displaying the seal continue to abide by their privacy policies and that those policies continue to be consistent with its principles. These periodic reviews may include, but are not limited to, auditing, random reviews, use of "decoys" or use of technology tools as appropriate to ensure that sites are adhering to the articulated privacy policies.

In cases where there is evidence that the company is not abiding by its privacy policies, the seal provider should establish clear criteria for placing that company on probation or beginning procedures for the seal's revocation. The seal provider should establish clearly defined criteria for when and how a company's seal may be revoked. A company should be given notice and the opportunity to request outside review before its seal is revoked. Seal revocation should be a matter of public record. The seal provider must clearly state the grounds for revocation and establish a post-revocation appeals process. In addition to the above criteria, the seal provider should also strive to ensure the integrity of the seal by monitoring for misuse or misappropriation.

Consumer Complaint Resolution

An effective third-party enforcement mechanism must provide its participants and consumers a structure to resolve complaints and consequences for failure to do so. Thus, a seal program must define the scope of complaints subject to the complaint resolution process, have a system in place to address complaints, the necessary staff to handle the volume of complaints and the organizational depth to resolve them. The seal program must provide a variety of easy mechanisms to allow consumers to lodge complaints or ask questions. Seal recipients must agree to the complaint resolution procedure.

Under the complaint resolution system, consumers must first be required to seek redress for their complaints from the company they believed to have aggrieved them, before being granted access to the seal program's complaint resolution mechanism. Where complaints cannot be adequately resolved by the company, and where the consumer and company have exhausted good faith efforts to reach agreement, the company should be required to submit to a complaint resolution mechanism.

Complaint resolution outcomes must not be contrary to any existing legal obligations of the participating company. Failure of a company to agree with the outcome of the seal program's complaint resolution should result in previously identified consequences to the company. Notwithstanding the complaint resolution process, the consumer, the company and the seal provider may pursue other available legal recourse.

Education and Outreach

A seal program must develop and implement policies to educate consumers and business about online privacy.

A seal program must develop and implement policies to encourage awareness of the program and online privacy issues with both consumers and businesses. Such techniques shall include: publicity for participating companies, public disclosure of material non-compliance or seal revocation, periodic publication of the results of the monitoring and review procedures, or referral of non-complying companies to the appropriate government agencies.

online privacy alliance

An alliance of global companies & associations
committed to promoting privacy online.

Online Privacy Alliance Association Policy

An association that joins the Online Privacy Alliance agrees to:

- endorse the Alliance mission statement, including: 1) adopting and posting privacy guidelines consistent with the Alliance's guidelines and appropriate to the association's membership; and 2) participating in self-regulatory enforcement mechanisms appropriate to the association's online activities;
- encourage its members to adopt privacy guidelines consistent with the Alliance's guidelines and appropriate to their industry's sector, and to implement appropriate self-regulatory mechanisms; and
- actively participate in the Alliance's business outreach and consumer education programs.

An association also may administer a seal or other third-party self-regulatory enforcement program at its discretion.

Other Materials

- Privacy Initiatives by Private Sector: A partial review of steps which OPA Supporters have done to help foster consumer confidence by protecting personal privacy in cyberspace.
  See http://www.privacyalliance.org/resources/privinit.shtml

- A Quick Guide to Helpful Tips and Technical Tools for safeguarding your privacy online.
  See http://www.privacyalliance.org/resources/rulesntools.shtml

- The OPA White Paper details a "layered" approach to privacy protection. The paper describes how the enforcement of existing laws by government, combined with industry self-regulation, creates "adequate" safeguards for the protection of personal information collected online in the United States.
  See http://www.privacyalliance.org/news/12031998-5.shtml

- The OPA Commentary document gives background on the development of the OPA Guidelines.
  See http://www.privacyalliance.org/news/12031998-4.shtml

FIP (Fair Information Practices)

FIP (Fair Information Practices) is a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. Different organizations and countries have their own terms for these concerns - the UK terms it "Data Protection", the European Union calls it "Personal Data Privacy," and the OECD has written *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which states these principles:

Simpli

a web solution with the accent on ease

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 in accordance with the Purpose Specification Principle 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.

These principles are reprinted from http://www.junkbusters.com/ht/en/fip.html#OECD under the terms of the GNU General Public Licence.

Selected Links

- OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data is available.
- Junkbusters on FIP has more information.

Assistance by: Simon Smith
Last update: September 12, 1999

HOME whatis?com HOME

Copyright © 1996-2000 TechTarget.com, Inc. All rights reserved.

Mr. HORN. And now our next individual is Solveig Singleton, director of information studies for the CATO Institute.

You might tell in a little description what the CATO Institute is.

Ms. SINGLETON. Sure, I will. Thank you, Mr. Chairman.

I'm Solveig Singleton, director of information studies at the CATO Institute, which is a free market or libertarian think tank based in Washington, DC. My area of expertise includes the Internet and telecommunications regulation. My testimony today is intended to illustrate how a privacy commission as proposed in H.R. 4049 can be of help to Congress in understanding privacy in the big picture in this country.

There are many privacy issues that come before Congress piecemeal, and Congress is well-adapted to hearings on specific topics like medical legislation or financial privacy and so on, but Congress rarely has the leisure to sit back and consider a comprehensive view of privacy overall across the economy.

Let me talk now a little bit about one of the questions I think would be important for the Commission to consider. I think the Commission could play a vital part in increasing Congress' understanding of how the increased use of government databases, new surveillance techniques and so on ultimately will affect the relationship between the U.S. citizens and their government.

Just in the past decade alone, we've had several new Federal databases created. I'll just run down some of these quickly. There's a National Directory of New Hires intended to enforce child support orders, but, of course, everybody ends up in it, not just parents. There's a new employment database for the Workforce Investment Act, a national medical database with proposed unique health identifiers, and there's a National Center for Education Statistics. On top of that, there's been various proposals for monitoring and tracing citizens' activities such as FIDNET, Federal mandates for driver's licenses, and an employment eligibility confirmation pilot proposal from the Immigration and Naturalization Service.

Now, each of these databases and each of these proposals comes along with good intentions, but the concern overall is that ultimately what we may see in this country is the right to work, the right to travel, the right to seek medical attention, the right perhaps to consult a lawyer in confidence, that these things are gradually transformed into privileges that are enjoyed only by those people who have their paperwork in order. And most Americans, I think, have better things to do than wanting to be thinking about whether their paperwork is in order all the time. People lose things, mistakes are made by clerks and so on. So I think a privacy commission would be ideally situated to look at these developments in the big picture.

Second, I think a commission could add substantially to Congress's understanding of the use of information about consumers by private sector businesses. Now, those of you who have heard me testify on Internet privacy will know I think many concerns about business use information are overstated. I basically think private businesses, they are either going to sell you something or not sell you something. I think that when it's a legitimate business that consumers need to be protected from, that the need for protection for consumers is fairly limited. But nevertheless, new tech-

nology makes people uneasy, and there's a danger that Congress will face tremendous pressure to move forward on privacy before they entirely understand the economic consequences of regulation.

In particular there's been a lot of opinion, including my own, brought forward in testimony, but very little actual factual information about the way information is used in the economy, what it means to businesses in terms of keeping costs down, what it means to consumers in terms of getting information about new products, new businesses, new services, and in particular there's little hard information about the impact of privacy regulation on small businesses including Websites, startups of any kind, charities and grass-roots political groups, many of whom trade actively in lists of information about donors or subscribers in order to get their foot in the door of civil society.

Third, a really critical issue, and where there is a real danger to consumers, is in the area of fraud and identity theft. There's some serious questions that need to be asked about the best approach to fraud and security issues. Is it to have less information circulating through the economy as a whole, or is it, in fact, to have more information about people of a kind that is easier to verify, such as digital signatures? In some cases the use of biometric identifiers like fingerprints might be appropriate. And finally, I think the most important question of all is how can law enforcement be more effective in enforcing existing laws against fraud and identity theft? A lot of these questions may be enforcement questions rather than questions of new laws or new policies being needed.

So to conclude and second the comments of some of the other panelists, I note that I think the proper role of the Commission would be to provide balanced and objective analysis and scholarship to fill gaps in our understanding of the complexities of privacy. I think in particular it might be valuable to have the Commission have the authority to contract with a group—a reputable group, an independent group of economists to come up with something like a cost-benefit analysis of different types of proposed regulation.

With that I conclude.

Mr. HORN. We thank you. Those are some very helpful suggestions.

[The prepared statement of Ms. Singleton follows:]

Singleton

Questions for the Proposed Privacy Commission

Testimony
Solveig Singleton
Lawyer, The Cato Institute
1000 Massachusetts Ave NW
Washington, DC 20001
(202) 842-0200

Before the

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

Hearing, May 16, 20000

Mr. Chairman, my name is Solveig Singleton and I am a lawyer and the director of information studies at the Cato Institute. Thank you for this opportunity to comment on the idea of a privacy commission. My testimony will examine the role such a commission would play in the debate about privacy. I will offer several important issues as examples of important contributions that such a commission might make. These will include:

- A review of how the vast amounts of information requested by the federal government can affect our rights to travel and work, and how to prevent abuses.
- How to apply the Fourth Amendment of the U.S. Constitution, which describes lawful searches and seizures, to new computer and wireless communications networks.
- In the private sector, the impact of broad privacy legislation or regulation on small businesses, consumers, charities, and grassroots groups.

Privacy, The Federal Government, and the Fourth Amendment

Government has unique powers of investigation, arrest, and trial that the private sector lacks. These unique powers make the possession of information by government fundamentally alarming in a way that uses of information in the private sector are not. This century alone contains far too many examples of governments--including our own--that have abused information they were entrusted with.

Just in the past decade, massive government databases have grown up. Beyond the census, social security, and the Bank Secrecy Act, there's a National Directory of New Hires with everyone in it (child support), federal mandates for drivers' licenses and birth certificates, pilot programs for "employment eligibility confirmation" (immigration), the evolution of the social security card into a de facto national identifier, a new employment database for the Workforce Investment Act, a national medical database with unique health identifiers, and the National Center for Education Statistics. On top of those new databases have come new proposals for monitoring and tracing citizen's activities, such as FIDNET.

A privacy commission could play a vital part in increasing Congress's understanding of how government information gathering and surveillance affects U.S. citizen's freedoms to work and travel, seek medical treatment, or exercise other rights overall. Most data-collecting proposals come with benefits attached--Aid to Families with Dependant Children, immigration law enforcement, or proposals to enforce child support orders--and each proposal standing alone seems well-intentioned enough on its face. But must we treat everyone like a deadbeat dad in order to catch a few wrong-doers? Will more government demands for information and identification turn holding a job or moving from state to state into a privilege enjoyed by those

with the right paperwork? This is the kind of question that a privacy commission would be ideally situated to investigate, to consider the implications of these databases as a whole, rather than in a piecemeal fashion.

Second, there is the question of whether the means by which information is collected is consistent with the Fourth Amendment. The Fourth Amendment of the United States Constitution provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Today, however, some police practices, such as the aggressive "stop and frisk" searches used on the occasion of the death of Amadou Diallo in New York City, seem to bypass this showing of probable cause. Some have proposed to allow "surreptitious" searches of homes for encryption keys. The "Know Your Customer" rules that the FDIC formally proposed--and backed down from--just last year remain in place as informal agency guidelines followed by many banks. The brunt of careless or unconstitutional searches will be borne, as always, by those least able to defend themselves--immigrants, small businesses, and minorities.

A privacy commission could provide much-needed perspective on an age when law enforcement has access to satellite photos, infrared, plaint-text readers, and many other surveillance data. The commission might be asked to study the application of the Fourth Amendment to police practices, business records, and new computer networks. The commission could also provide valuable information about alternatives law enforcement techniques (such as the use of informants) that do not jeopardize the safeguards provided by the Fourth Amendment.

Data Protection and the Private Sector

A privacy commission could also fill significant holes in Congresses understanding of another completely different aspect of privacy, the use of information about consumers by private sector businesses. Private sector businesses have little power to violate citizen's rights with the information they hold; consumers do not need to be protected from people trying to invent and sell goods and services. Nevertheless, the use of consumer information by the private sector has become controversial. Horror stories and consumer surveys have taken the place of leadership from legislators. There is some danger that broad legislation or regulation could be passed with bizarre and painful consequences for the information economy.

For example, little information is available on the probable impact of privacy regulation on small businesses (including web sites), startups, charities, and grassroots groups. The experience of Europe with privacy regulation suggests that regulation makes the kind of information that these groups use to get their foot in the door of civil society much less readily available, and much more expensive than when information flows freely throughout the economy.

In addition, a privacy commission should ask how privacy regulation would effect the availability of products, services, and information to consumers. Information about the impact of such regulation on the prices and selection of goods and services to consumers is vitally needed, and this information cannot be provided by shallow surveys of web policies or public opinions.

Finally, a privacy commission should consider how to best defend consumers from real dangers such as identity theft and fraud. Treating legitimate businesses like stalkers is not the

answer. Would the use of biometric identifiers like voiceprints or fingerprints help businesses with security concerns? How can law enforcement be more effective in enforcing existing laws against fraud and identity theft?

Conclusion: The Need for a Balanced and Scholarly Commission

A privacy commission could play a vital role in informing Congress, and, ultimately, the American public, about the changing relationship between the federal government and its citizens that comes with the growth of federal databases and investigative powers. This "Big Picture" of this issue has never been addressed. Databases and powers of search and seizure have grown up on a piecemeal basis. But Congress would be right to ask whether the result has has been a systemic shift in the powers of government with relation to the people.

Likewise, a privacy commission could play a very important role in ensuring that Congress does not adopt radical proposals to regulate private-sector uses of information without fully understanding their economic consequences. The usual rule for people interacting with one another is that each is free to learn from the other, and make free use of the knowledge gained in the exchange. That is how the economy has long operated (with a few exceptions). Abandoning the free flow of information is a truly drastic measure, and should not be considered without a complete understanding of its economic impact.

My primary misgiving about the idea of a privacy commission is that its work cannot provide a solid foundation for Congressional understanding of these issues unless the commission is balanced. It is easy to imagine a commission composed mainly of a bunch of the usual suspects with an agenda, with little new to offer in terms of serious analysis of privacy

issues. In my view, the proper role of a commission would be to provide objective analysis and scholarship--the politics is for Congress. It might help to limit such a commission's role to that of a fact-finder, for example, rather than asking that its primary role be to recommend one policy over another.

Mr. HORN. Mr. Ron Plesser is legislative counsel to the 1977 Privacy Commission. Mr. Plesser.

Mr. PLESSER. I think I was general counsel, but "was" rather than "is."

Good afternoon, Mr. Chairman, members of the committee, and thank you very much for the opportunity to appear before your subcommittee as it examines the creation of a commission for the study of privacy protection. My name is Ronald Plesser, and I'm partner in the law firm of Piper Marbury Rudnick & Wolfe, and I chair their Electronic Commerce and Privacy Group. I served as general counsel for the Privacy Protection Study Commission for the entire life of the Commission from 1975 to 1977, and most recently I've served along with Mary Culnan on the Federal Trade Commission's Advisory Committee on Online Access and Security.

I'm pleased to appear before you today to share my experiences as a staff member of the first and only Privacy Commission and to comment on H.R. 4049 and the potential establishment of a new privacy commission.

Created by the Privacy Act of 1974, the Privacy Protection Study Commission was directed by Congress to make a study of, quote—study of the data banks, automatic data processing programs, and information systems of governmental, regional, and private organizations in order to determine the standards and procedures in force for the protection of personal information. The Commission also sought to examine the balances between legitimate and at times competing interests of the individual, the information system and society in general.

I would like to point out, as I think others have, that we issued our report in 1977, which actually was the first year that the personal computer was commercially available. So there's obviously been a world of development and shift since then, but I think their basic principles may have stayed more the same than we could have imagined. The Commission recommended ways of providing additional protection for the privacy of individuals while meeting society's legitimate need for information.

The Commission based its recommendations on the conclusion that effective privacy protection must have three concurrent objectives: one, minimize intrusiveness in the lives of individuals, and this relates really to a large extent to government issues; maximize fairness in institutional decisions made about individuals—this is the famous fair information practice principles; and provide individuals with legitimate, enforceable expectations of confidentiality.

One of the critical findings of this report was that privacy needs to be addressed on sector-specific basis, given that there are different concerns raised by different information systems. The Commission felt that the historic development of privacy protection as well as the then current realities required that each be dealt with separately.

The Commission explicitly rejected a proposal for an omnibus privacy statute establishing government authority to regulate the flow of all personal information. This rejection was based on several considerations, including the danger of government control over the flow of both public and private information, the greater influence on the private sector than the public sector of economic in-

centives that encourage voluntary compliance with principles, and three, the difficulty of legislating a single standard for widely varying recordkeeping practices in the private sector.

I would like to highlight a few areas of the particular bill you're looking at that I believe could pose obstacles to the effective service of a commission based on my practical experience. First, the Commission envisioned by the bill is comprised of too many members. It was critical that there were seven members of the Commission as compared to the 17 recommended by H.R. 4049. Broad representation of various interests on the Commission is an important goal. However, for management reasons and to enable group consensus, it is important that the Commission be limited to a smaller number.

The second point, the Commission's effort needs to be sufficiently funded to allow for careful, balanced investigation. H.R. 4049 allocates $2.5 million in the year 2000, and you may be interested to know that that's exactly the same amount of money that the Privacy Commission got in 1974, and while we, I think, felt that was a fully sufficient amount of money back in 1974, we had 60-some-odd days of hearings and other stuff. I think that amount is woefully inadequate for an adequate study today.

I've hit my time, and I wondered if I could have just another minute to say that I think there are competing reasons for and against the Privacy Commission. On one hand, I agree with what everyone has said about the complexity of the issue and that it needs additional study. Whether that initial study has to be done by a new independent commission, or it can be done by existing authorities I think is an issue.

I'm also concerned—I was very involved with the Children's Online Privacy Protection Act representing several clients, and I think we came out with a very balanced piece of legislation that was supported by government, public interest groups, the private sector and, of course, Congress. I wonder if we could have developed something as carefully tuned and balanced as a result of a commission process, or if it worked just as well by having inquiry by Congress without having the added kind of exposure and publicity that would be involved in a commission. I think there are positions on both sides of it. I certainly support Christine Varney's point of view on the need to have a commission, but I think we should look at it very carefully as we go forward. Thank you.

Mr. HORN. Thank you very much. Those are very helpful suggestions.

[The prepared statement of Mr. Plesser follows:]

BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

HEARING ON H.R. 4049
ESTABLISHING A COMMISSION FOR THE
COMPREHENSIVE STUDY OF PRIVACY PROTECTION

May 16, 2000

TESTIMONY OF RONALD L. PLESSER

Ronald L. Plesser
Piper Marbury Rudnick & Wolfe LLP
1200 Nineteenth Street N.W.
Washington, D.C. 20036
202/861-3900

Plesser

Introduction

Good morning, Mr. Chairman, and thank you for the opportunity to appear before your Subcommittee as it examines the creation of a commission for the study of privacy protection. My name is Ronald Plesser and I am a partner at the law firm of Piper Marbury Rudnick & Wolfe LLP. By way of a brief introduction to my experience in the privacy arena, I represent many companies on a wide array of privacy-related issues, including health care, financial, children, Web site, wiretap and cable privacy, as well as European and other international privacy matters. I have been actively involved in state, federal, and international legislative initiatives as well as self-regulatory efforts in these areas for many years. I work extensively with various trade associations and "dot-com" companies to develop and implement fair information policies and practices. In addition, I coordinate a group of the leading information industry companies that provide services to help identify, verify, or locate individuals. I worked with this group to develop and adopt self-regulatory principles governing the collection, use and dissemination of personal information.

I served as general counsel to the Privacy Protection Study Commission for the entire life of the Commission from 1975 to 1977. In addition, I served on the Clinton-Gore transition team on Telecommunications, participated as the industry representative in the U.S. delegation to the OECD on Consumer Protection in the Global Electronic Environment this past year, am currently on the coordinating committee of the Online Privacy Alliance (OPA), and also serve on the Federal Trade Commission's (FTC) Advisory Committee on Online Access and Security.

I am pleased to appear before you today to share my experiences as a staff member of the first and only Privacy Protection Study Commission, and to comment on H.R. 4049 and the potential establishment of a new privacy protection study commission.

Because there has been heightened attention to privacy in recent years, this issue has been deemed a top priority by government and industry alike. In seeking to address the privacy issue as it emerges in a variety of different settings, it becomes immediately evident that privacy protection is a complex task because the requirements are never static and the issues are multi-faceted. Privacy issues have always involved a careful weighing of a multitude of factors in efforts to strike the appropriate balance between individual privacy interests and important and socially beneficial uses of information. An examination of privacy protection necessarily involves assessing and reassessing the interplay between technology and privacy in light of developments that have a major effect on the collection, use, and disclosure of individual information in the global information economy. In viewing privacy against this backdrop, the Privacy Commission's report, although issued in 1977, still has validity, offering many lessons both in terms of the substantive findings articulated in the report as well as in the process involved in its creation. I now would like to share with you some of these lessons.

The Privacy Balance

Created by the Privacy Act of 1974, the Privacy Protection Study Commission was directed by Congress to make a "study of the data banks, automatic data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information." The Commission sought to examine the balance between legitimate and, at times, competing interests of the individual, the information system, and society in general.

The Commission recommended ways of providing additional protection for the privacy of individuals while meeting society's legitimate needs for information. The Commission based

its recommendations on the conclusion that effective privacy protection must have three concurrent objectives:

- minimize intrusiveness in the lives of individuals;
- maximize fairness in institutional decisions made about individuals; and
- provide individuals with legitimate, enforceable expectations of confidentiality.

One of the critical findings of this report was that privacy needs to be addressed on a sector-specific basis given that there are different concerns raised by different information systems. The Commission felt that the historical development of privacy protections as well as the then-current realities required that each area be dealt with separately.

The Commission explicitly rejected a proposal for an omnibus privacy statute establishing governmental authority to regulate the flow of all personal data. This rejection was based on several considerations, including: (1) the danger of government control over the flow of both public and private information; (2) the greater influence on the private sector than on the public sector of economic incentives that encourage voluntary compliance with privacy principles; and (3) the difficulty of legislating a single standard for widely varying record-keeping practices in the private sector.

The standards applied to the various record-keeping relationships in the private sector have emerged from sharply focused legislative inquiries that identify problems arising in particular record-keeping relationships. By considering the distinct roles played by specific types of records in the lives of individuals, and the nature of the harm caused by their misuse, Congress and state legislatures have been able to balance the privacy interests at stake against the public interests that are served by the use of personal data in various contexts.

The Evolution of the Information Age

It is important to remember that when we wrote the report in 1977 we were living in a very different age. It is hard to believe that more than 20 years have passed and we are now into a new millennium. We had just passed the bicentennial at the time the report was released, and we were only embarking upon the advent of the personal computer. In our survey of the privacy landscape, we looked at large computing systems with centralized databases rather than the distributed network capacities of the modern era. While the information age was being speculated on, no one dreamed that the Internet and the World Wide Web would become as pervasive as they are today.

Although we are living in a vastly different era, one bedrock of privacy protection still predominates. That is, that in addressing the privacy issue we need to balance an individual's privacy and the need for government and the private sector to use and maintain information in ways that further societal interests. U.S. privacy laws have continued to advance these objectives through the further development of the sector-by-sector approach to data privacy, which accounts for the sensitivity of the personal data and whether it is likely to be used in a way that could adversely affect the data subject.

Practical Experiences

I would like to highlight a few areas of the bill that I believe could pose obstacles to the effective service of a commission based on my practical experiences. First, the commission envisioned by the bill is comprised of too many members. It was critical that there were seven members on the Commission as compared to the 17 recommended by H. R. 4049. Broad representation of the various interests on the commission is an important goal. However, for

management reasons, and to enable group consensus, it is important that the commission be limited to a smaller number. Second, the commission's effort needs to be sufficiently funded to allow methodological and balanced investigations. H.R. 4049 allocates only $2,500,000, which is about the same amount of money allocated for the study in 1974. It is important that sufficient resources are allocated to ensure that factual research, hearings, and transcripts all are part of the effort of the privacy commission.

Conclusion

There are competing reasons both for and against creating a new privacy commission. On the one hand, I recognize the complexity of the privacy issue and appreciate the fact that this issue deserves a thorough examination so that appropriate balances can be struck to perpetuate the American privacy values and principles which have developed. In addition, the creation of a commission is a better option than broad legislation that does not further the sectoral approach to privacy protection.

On the other hand, I do have significant reservations about establishment of a commission because its characterization of the issues likely would receive a great deal of attention and scrutiny, which could distort the privacy issue and undermine much of the promise and value of responsible information policies and practices. Such potential hype would not result in good public policy. In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA) with broad support from industry and consumer interests. This statute was written without a study commission and reflects a good piece of legislation that carefully addresses real problems.

I commend the Committee on its thoughtful inquiry into this important issue and its efforts to further the dialogue on privacy.

Mr. HORN. Our last witness on this panel is Stanley Sokul, member of the Advisory Commission on Electronic Commerce. Why don't you tell us a little bit about that advisory commission.

Mr. SOKUL. Thank you. Thank you for inviting me to testify today. As you noted, I served as a member of the Advisory Commission on Electronic Commerce, which studied the issues surrounding Internet taxation. We issued our report on April 12, and our tenure expired on April 21.

I'm here primarily to urge you not to neglect the privacy implications of Internet taxation, but would also like to offer some suggestions on a potential privacy commission based on my Tax Commission experience.

If a commission on privacy is created, I hope the subcommittee will consider an issue that the Tax Commission uncovered but did not resolve. In order for States to effectively collect taxes on Internet sales transactions, the sales need to be identified on an individual basis. Such government tracking of consumers' Internet purchases could have significant privacy ramifications. The most striking example involves the types of privacy invasions that would have to occur for States to track and tax the purchase of digital goods.

The Internet privacy debate generally focuses on the activities of private entities, how companies compile on-line purchase information and even track Web surfing for commercial purposes. The debate revolves around the nature and extent of consumer access to and control over the collection and use of such information; for example, should an opt-in or opt-out requirement be imposed on Internet data gathering and sharing.

In contrast, imposing a national system to collect State sales taxes raises the specter of the government tracking individual purchase information. In this environment, the consumers would have no control. The only way for consumers to opt out of the government tracking their purchase activity would be to forego the Internet purchase altogether.

During the Tax Commission process, the State and local organizations proposed a Streamlined Sales Tax System for the 21st century. This system would insert a new layer of requirements into electronic sales transactions, a national clearinghouse or database, to track Internet purchases so the proper tax could be calculated, levied, and remitted to the proper jurisdiction. This proposal raised some significant privacy concerns, and ultimately the States stopped advocating the system as a solution, at least before our Commission.

The effects a new Internet sales tax collection regime would have on consumer privacy and thus Internet commerce remain unexplored. Confronted with many concerns but few details, the Tax Commission adopted a resolution I authored to recommend that Congress study the privacy implications of Internet taxation very carefully. It was one of the few items that attained a two-thirds supermajority vote to constitute a formal recommendation to Congress. We recommended that Congress explore privacy issues involved in the collection and administration of taxes on e-commerce, with special attention given to the repercussions and impact that any new system of revenue collection may have upon U.S. citizens.

Accordingly, because the Privacy Commission may be a key vehicle through which Congress explores Internet privacy issues, I would urge that the privacy implications of Internet taxation be added to the Commission's agenda.

Finally, I would like to comment briefly on two problems that the Tax Commission confronted. First, our Commission lost nearly half of its 18-month tenure due to an appointment controversy. The statute required equal representation from State and local interests and business interests and gave the House and Senate leaders a fixed number of appointments. When all the appointments were announced, a statutory balance had not been achieved, and the imbalance took 8 months to sort out.

H.R. 4049 as presently written provides leadership with specific appointments, but does not specify that certain interests must be represented on the Commission. If the subcommittee ultimately decides to list different interests that should be represented, I would suggest that you carefully account for what will occur if the initial round of appointments fails to fulfill the representational requirements.

Second, the Tax Commission operated under a two-thirds supermajority requirement to report findings and recommendations to Congress. H.R. 4049 presently contains only a simple majority requirement. I would urge you to consider a supermajority provision. While the Tax Commission did not ultimately achieve a two-thirds result for the bulk of its report, and that failure created some controversy, I believe still that the requirement created a healthy dynamic within the Commission that encouraged the opposing interests to work together. However, if you institute a supermajority provision, the statute must be clear that a lack of one does not negate the need to file a report.

Thank you again for the opportunity to testify, and I'll be happy to answer any questions.

Mr. HORN. Well, thank you.

[The prepared statement of Mr. Sokul follows:]

HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

Testimony of Stanley S. Sokul
Davidson & Company, Inc.
1101 Pennsylvania Avenue, NW, #810
Washington, D.C. 20004
(202) 638-1101

May 16, 2000

Thank you for the opportunity to testify today. As you know, I served as a Member of the Advisory Commission on Electronic Commerce, which studied the issues surrounding Internet taxation. We issued our report on April 12, 2000, and our statutory tenure expired on April 21, 2000. I am here primarily to urge you not to neglect the privacy implications of Internet taxation, but would also like to offer some suggestions for the privacy commission based on my tax commission experience.

The privacy issues raised by the Internet are just as complex and confusing as the tax issues. As with taxes, offline privacy rules and expectations do not necessarily translate well to the Internet environment. Furthermore, different rules may exist for different situations. Three different federal agencies – the Departments of Treasury and Health and Human Services, and reportedly the Federal Trade Commission – are currently working on new privacy rules in their respective spheres. They have unlikely consulted with each other, however, to see if consistency is possible or even desirable. A commission process is an understandable means of sorting through the present confusion.

Privacy and Internet Taxation

If a commission on privacy is created, I hope this subcommittee will consider an issue that the Advisory Commission on Electronic Commerce uncovered, but did not resolve. In order for states to effectively collect taxes on Internet sales transactions, the sales need to be identified on an individual basis. Such government tracking of consumers' Internet purchases could have significant privacy ramifications. The most striking example involves the types of privacy invasions that would have to occur for the states to track and tax the purchase of digital goods.

The Internet privacy debate generally focuses on the activities of private entities – how companies compile online purchase information, and even track Web surfing, for commercial purposes. The debate revolves around the nature and extent of consumer control over the collection and use of such information – for example, should an opt-in or opt-out requirement be imposed on Internet data gathering and sharing activity.

In contrast, imposing a national system to collect state sales taxes raises the specter of *the government* tracking individual purchase information. In this environment, the consumers would have no control. The only way for consumers to "opt out" of the government tracking their purchase activity would be to forego the Internet purchase altogether.

During the tax commission process, the state and local organizations proposed a "Streamlined Sales Tax System for the 21st Century." This system would insert a new layer of requirements into electronic sales transactions – a national clearinghouse or database – to track

Internet purchases so that the proper tax could be calculated, levied and remitted to the proper state. These new clearinghouses were labeled "Trusted Third Parties." This Trusted Third Party system raised some significant privacy concerns, and ultimately the states stopped advocating the system as a solution before the Commission.

The effects a new Internet sales tax collection regime would have on consumer privacy and thus Internet commerce remain unexplored. Confronted with many concerns but few details, the tax commission adopted a resolution I authored to recommend that Congress study the privacy implications of Internet taxation very carefully (attached). This resolution was one of the few items that attained a 2/3rds supermajority to constitute a formal recommendation to Congress. We recommended that Congress "explore privacy issues involved in the collection and administration of taxes on e-commerce, with special attention given to the repercussions and impact that any new system of revenue collection may have upon U.S. citizens…, " and that Congress "[t]ake great care in the crafting of any laws pertaining to online privacy (if such laws are necessary) to avoid policy missteps that could endanger U.S. leadership in worldwide e-commerce."

Accordingly, because the privacy commission may be a key vehicle through which Congress explores Internet privacy issues, I would urge that the privacy implications of Internet taxation be added to the commission's agenda.

Drafting Issues

Finally, I would like to comment briefly on two problems the tax commission confronted. First, our commission lost nearly half of its eighteen-month tenure due to an appointment controversy. The statute required equal representation from state and local interests and business interests, and gave the House and Senate Leaders a fixed number of appointments. When all the appointments were announced, the statutory balance had not been achieved, and the imbalance took eight months to resolve.

H.R. 4049, as presently written, provides Leadership with specific appointments, but does not specify that certain interests must be represented on the commission. Some tension exists here because balanced representation will help give credibility to the commission and its work. If the subcommittee ultimately decides to list the different interests that should be represented, I would suggest that you carefully account for what will occur if the initial round of appointments fails to fulfill the representational requirements.

Secondly, the tax commission operated under a 2/3rds supermajority requirement to report "findings and recommendations" to Congress. H.R. 4049 presently contains only a simple majority requirement. I would urge you to consider a supermajority provision. While the tax commission did not ultimately achieve a 2/3rds result for the bulk of its report (the privacy recommendation did attain 2/3rds status), the requirement created a healthy dynamic that encouraged the opposing interests to work together – and we came very close to achieving a supermajority result.

The tax commission resolved down to three basic interest groups, and the privacy debate potentially has many more interests at stake. This could be an advantage to the privacy commission, as there could be a lower likelihood of polarization and thus stalemate by a determined minority. I believe the 2/3rds requirement was very constructive for the tax commission, and could be for the privacy commission as well. If you institute a supermajority provision, the statute must be clear that a lack of one does not negate the need to file a report.

Thank you again for the opportunity to testify, and I would be pleased to answer any questions you may have.

THE ADVISORY COMMISSION ON ELECTRONIC COMMERCE
RECOMMENDATION ON PRIVACY

G. Privacy Implications of Internet Taxation

The issue of consumer privacy is one that pervades all aspects of e-commerce.

The Commission process has shown that proposals to increase state and local authority over the taxation of e-commerce have significant privacy ramifications.

Furthermore, technological advances will likely allow for increased tax collection efficiencies, however other important principles — such as increased exposure of individual privacy — must be balanced against what is technologically possible.

The issue of consumer privacy is one that pervades all aspects of e-commerce, and not just the tax administration system.

Recommendations: Privacy

• Explore privacy issues involved in the collection and administration of taxes on e-commerce, with special attention given to the repercussions and impact that any new system of revenue collection may have upon U.S. citizens and the steps taken in systems developed to administer taxes on e-commerce to safeguard and secure personal information.

• Take great care in the crafting of any laws pertaining to online privacy (if any such laws are necessary) to avoid policy missteps that could endanger U.S. leadership in worldwide e-commerce.

Votes on Adoption: 16 Yeas, 1 Abstention, 2 Not Present

The proposal passed by more than 2/3rds (16) and is considered a finding or recommendation.

Advisory Commission on Electronic Commerce, Report to Congress, page 37 (April 2000)

Mr. HORN. And we will now go to questions, and we'll start with—we're going to do it 5 minutes each side, everybody, so we all get into this and rotate it a few times. So I'm going to yield my time to the gentleman from Arkansas Mr. Hutchison, 5 minutes.

Mr. HUTCHINSON. Thank you, Mr. Chairman. I want to thank each of the witnesses. That was outstanding testimony, very thoughtful, and with your background and expertise, I think it is very helpful to the committee.

First, Mr. Belair, I don't think you recounted a little bit of your background on privacy. Could you do that for the committee? I know it's in your written material, but could you elaborate?

Mr. BELAIR. I'm happy to do it. I'm editor, along with Alan Westin, which—of Privacy & American Business, which is a not-for-profit, privacy-friendly, business-sensitive publication. I also have a privacy consulting firm with Alan Westin, and I'm partner in a law firm, Mullenholz, Brimsek & Belair, and my practice there is all privacy-related. I was deputy general counsel of the White House Privacy Committee in the Ford administration. I said that the other night at the supper table, and one of my teenagers said, the Ford administration, God, you're old, and I guess that's probably right. I've also been the general counsel of the National Commission on the Confidentiality of Health Records and represented a number of other both public sector and private organizations.

Mr. HUTCHINSON. I think that's extraordinary background, and your testimony was that you supported the Privacy Commission creation.

Mr. BELAIR. That's correct. I think it's—I not only support it, I think it's really just the right thing at the right time. I think it's critical.

Mr. HUTCHINSON. Dr. Culnan, you have raised some good points. I thank you for your support for the legislation as well, but you raised the concern about balancing the Commission, and you heard the comments from our last witness. Could you help us here as to what your suggestion is on how to balance the Commission? Let me tell you, first of all, some of the thinking in this that, one, it should be balanced. It's very important, and we want to get people who are open-minded and can promote a consensus. The option is, you know, to specify who all should belong to it or leave it to the political process, the people who are appointing, that you are going to pressure them, we are going to pressure them to appoint balanced people. I am open to any suggestions, but that was the thinking.

Ms. CULNAN. I think I would be against sort of a rigid set of standards saying you have to have X number of people that represent a certain point of view, but there might be a statement in the legislation that encourages or advises, I believe, the different people who are appointing Commissioners to consider diversity of perspectives in terms of doing that. One reason is because if it turns out the entire Commission is tilted toward a particular point of view, it will not have a lot of credibility, and there will be a lot of fighting and yelling about the kind of things that go on when you don't have multiple views reflected.

I also want to second Mr. Sokul's point about the appointment process. The commission I was on, a lot of people got tangled up in the appointment process, and I think that can do great det-

riment to the Commission if people don't get appointed quickly and get brought on board and the Commission gets off and running. We had to have half private sector and half Federal Government commissioners, and it took quite a while to locate the private sector people who were willing to serve.

Mr. HUTCHINSON. It shouldn't be as problematic if you do not specify all of the backgrounds necessary. I agree with you, and we've already half drafted some language that would talk about the broad interests that should be represented on it and the diversity of opinion reflected. I know I've raised—Ms. Varney, do you have any comment on this, and I also wanted to ask you specifically about your goal—or your statement that the goals of the Commission should be clearly articulated. Help me out here, again. The written copy I have did not elaborate all the things that you said so well.

Ms. VARNEY. Well, I can give you this as well. I guess my concern, Congressman, is that the privacy debate has generally been very polarized. There are a lot of thoughtful people, including people that you've heard from today and yesterday and will be hearing from, who really are looking for a balance.

What I would hate to see in the Privacy Commission is this division, this continued polarization. So if I could put my desires in writing in a preamble, it would be to really give the Commission guidance that its goal is to recommend to the Congress a comprehensive approach to privacy that balances the economic benefits of the free flow of information with the need for citizens to be able to protect their own personal privacy preferences.

Mr. HUTCHINSON. You think that language would be sufficiently instructive to the Commission?

Ms. VARNEY. I think it would help, because I think what we have seen in the privacy debate, this sort of view—a very stark view that either the use of information without very aggressive, very explicit consumer or patient or individual written affirmations and consents ought to be prohibited, and on the other side we've seen this view that all information flow in the commercial arena has some benefit, and therefore, anything that inhibits it is bad. That has really, in the short time I've been doing this compared with my colleagues—I only started dealing with this in 1994—that has really driven much of the debate. You don't find a lot of balance.

Mr. HUTCHINSON. My time has expired. Thank you, Mr. Chairman. Thank you.

Mr. HORN. We thank you.

Now I yield to the ranking member on the subcommittee who I believe will yield to the ranking member on the full committee.

Mr. TURNER. Thank you, Mr. Chairman. As you know, Mr. Waxman, our ranking committee member is here with us. Mr. Waxman has taken a great deal of interest in the subject of privacy, particularly in his work to try to establish protection of health information for all Americans, and I want to yield to him or ask the Chair to yield to him for the beginning of our round of questioning.

Mr. HORN. You can yield to him. Go ahead.

Mr. TURNER. Mr. Waxman.

Mr. WAXMAN. I thank both of you for allowing me to question the panel.

I want to thank the members of the panel for your testimony.

Mr. Plesser, let me start with you. You testified that you think 17 Commissioners is too great a number for reaching consensus. Do you have any recommendations on what would be an appropriate number of Commissioners to have and how to ensure that appropriate stakeholders are represented?

Mr. PLESSER. I was looking at it from the perspective of staff working with diversity. You have to understand that unlike a congressional committee, those members would not have their individual staffs. So all of the kind of briefing, just the mechanics of briefing and working with people to get them up to speed, to make the decisions to have 17 is quite a lot. I would think that single digit, 7, 8, 9, you have to decide the odd-even issue, but I would think something under 10.

I think the question of balance, frankly, being on the FTC Advisory Committee, I think you've got to go to 40, probably to the size that that went to, to make sure you had somebody from every sector, and even in that advisory committee that was 40, I think there probably were some people and some interests that felt that they weren't represented.

I think you really have to do what Christine has suggested, which is try to get some very well-balanced, centered people in the group, whether or not—you don't maybe try to get somebody from the consumer group and the business group and this group, but get people—certainly some academics, some people who have been thoughtful on the issue, and I think more kind of representatives more like we expect our Congress people to exercise good judgment rather than come from a specific point of view. But I think if you try to do 17, I just think we also—let's stay and talk about what happened at the Internet Tax Commission, but I think that when you have that large a commission representing specific points of view, it's going to deadlock, particularly in the situation where there's a supermajority vote.

I agree with Stan, I think supermajority is good, but 17—I'm a lawyer, but a lot of what I do is run coalitions, and 17 is a lot of people to get a good result with.

Mr. WAXMAN. I noticed other members of the panel are shaking their head in the affirmative, so they seem to agree with you about the size.

Let me ask you about the resources for such a commission. Dr. Willis Ware served as vicechair of the 1975–77 Privacy Protection Study Commission for which you were general counsel; stated in written testimony to the subcommittee that the Commission spent over $2 million, but just the effects of inflation over 25 years would make a realistic funding more like $4 to $5 million.

You mentioned in your testimony the importance of ensuring that the Commission would be provided sufficient resources. What do you think would be appropriate to meet the needs of a proposed privacy——

Mr. PLESSER. I'm totally unfamiliar with the current policies of GSA and how much space costs. That was an issue that shocked us, frankly, back in 1974 where a good part of our budget had to go to rent. I think the overhead issues like that I don't think any of us really think about. I think we had to rent furniture or had

some furniture charge. The government was very helpful in that we got a lot of people from different parts, HHS, HEW back in those days. We got a lot of loaners, and that helped us expand and encouraged the Commission to have loan personnel from certainly on medical records, to have some HHS people and stuff like that is very helpful and critical to the Commission.

I always agree with Dr. Ware, and so if he says $4 to $5 million, that sounds right, but I think my point is that there has to be some really serious fact-finding, some balanced hearings, an opportunity, as Mary suggested, for a lot of people to input. I want a smaller number of Commissioners, but I sure want it to have maximum outreach, and I think if you keep the funding down too low, which gets a lot of press releases and not a lot of careful investigations, I think you're either in it or not, but I think it would be difficult to cheap out.

I agree with Willis that 1974 and the year 2000, to fund something at the same level is not realistic on inflation.

Mr. WAXMAN. My time is up. I had other questions, but we'll get that to another round.

Mr. HORN. You may ask one more question.

Mr. WAXMAN. Let me ask Dr. Culnan what her thoughts are about the sufficient resources to meet the mandates of this bill, and what do you think we need to do to attract the high caliber of personnel—not personnel to work on it, but the members who actually serve on a commission?

Ms. CULNAN. The issue is can people balance—they must feel committed to serving on such a commission. Certainly if I were invited, I would make every effort to serve because it would be a tremendous honor to be asked. People need to feel, I think, that it's going to be an important, substantive commission that is going to yield a report that people are going to listen to; that it will be of the same stature as the 1977 report. That is an evergreen report. People still read and refer to that today 23 years later even though the technology is very different.

I also agree with Ron Plesser about appointing people who themselves represent balanced interests, which is probably a good way to deal with the diversity issue, as opposed to having people that have their feet planted in a particular point of view and are likely to dig in.

Mr. WAXMAN. Also people who are not going to give up their day jobs, because they are not going to be paid to serve on this. Is that going to be a problem for some of the people?

Ms. CULNAN. It may be a problem depending on the time constraints. If the 20-hearing rule is still in effect, and the Commissioners are supposed to fly around the country, that's going to take an enormous amount of time, and people will be probably giving up 1 or 2 weeks a month of their time to do this, let alone they also need to meet face to face to deliberate. They do need to have a chance to absorb testimony and information from a wide variety of experts and point of views and should use whatever is the best way is to do this.

I would also say even if you were to pay people, it's very difficult to find people who can take 18 months off from their job, people

who are willing to step off the fast track, and so I don't think that would necessarily be the solution either.

Mr. WAXMAN. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. We'll go to 6 minutes now for everybody.

Dr. Culnan, I'm curious. In your testimony you bring up the fact that there are few laws that protect personal information on Web databases. In your studies of the fourth amendment, what type of legislation do you think is needed for the Web databases?

Ms. CULNAN. I have not studied this yet, but it—people have raised this as an emerging issue in the future that we need to look to. One of the issues I raised in my testimony is that we be sure not to try to understand what may happen in the future by looking in the rear-view mirror, and cited the issues related to balancing national security interests versus civil liberties in the area of protecting critical infrastructures and the issues that when people put their personal information in a database that's not stored on their personal computer, but is on somebody else's server, that is raising new issues that haven't been addressed, and hopefully the Commission would look to some of these future and emerging issues as well as the issues we're grappling with today.

Mr. HORN. Do you or any of the other presenters know people that are working on the fourth amendment issue?

Ms. CULNAN. The Center for Democracy and Technology is very interested in this issue, and they are the ones who have brought it to my attention.

Mr. HORN. Let me move now to Mr. Belair. I've had an interest in the European situation for a number of years. I've been on the delegation of the Congress to the European Parliament, and we went over there just at the time when the Parliament had asked all the member countries to develop a privacy law. And the ones in the Polish Government had worked with us over here, and I'm sure they worked with some of you because they are very interested in what Americans develop in this area. And I was just curious what you feel, Mr. Belair, as to the impact of those policies on commerce, be it an American going to Europe or Europe going to America. I know they have got a moratorium on it for a while, but some of them in draft seem to be fairly rigid.

And I had suggested, because we happened to be visiting with the President and Prime Minister of France and Poland, I suggested that they put together a commission, in the case of Poland, of Polish companies that operate with subsidiaries in the United States and then same with America and American companies that operate in Poland; same with the President of France. They thought that was a fairly good idea to get some feeling as to what this really means when you have to relate it to industrial data moving across the Atlantic, and I wondered what you could educate us on, and do you feel that's a real problem? Will it become simply a nontariff trade barrier, for example?

Mr. BELAIR. Certainly has that potential. As you know, the Department of Commerce has been at work with the EU to agree on safe harbor accords, and they are close. Of course, they've been close now for many, many months. Assuming that safe harbor is negotiated, then I think we'll see some fascinating impacts here as

companies have a limited amount of time to decide whether they are going to subscribe to those safe harbor accords.

One of the things that the safe harbor accords do is bust through the sectorial industry-by-industry approach that we have always had and apply fairly generic privacy rules across the whole range of personal information.

That's No. 1.

No. 2, are we going to see a bifurcation where we've got some data that is subject to the safe harbor accords, namely data that's moved over from Europe, and then a second set of data that's domestic data that doesn't enjoy that kind of protection, or are we going to end up, as many of us think, with one approach, a global approach really, dictated to us by the Europeans?

Third, and then I'll stop, although obviously it's a topic that we could talk about for a long time, and that is that the Europeans clearly have not thought through what the impact is of the application of their rules in an on-line environment. They would argue, for example, that even a United States citizen who happens to be in France on a business trip and then pulls up on his screen a United States Web site and engages in some kind of a transaction that generates personal information, that information is subject not to United States law, but that's subject to the EU directive and, in this example I've just given, the French national law.

So it certainly does hold the potential for having an adverse impact on trade. I think—it's one of the things—the reason I mentioned it is I think it still remains to be seen how that sorts out.

Mr. HORN. I know there are scholars at the Brookings Institution that are working on this. Do you know where scholars are providing some initiative and some analysis of these different policies that are evolving in legislative committees in Europe? What's the best shot we can get from people in that area?

Mr. BELAIR. I think you're right, there's an awful lot of work and an awful lot of focus for a lot of groups back here and a lot of groups over there. Privacy & American Business, just to do a commercial since the segue is there, has a Web site, PrivacyExchange.org, and on that Web site is all of the latest information about the EU directive, about the national laws, about other national privacy laws, about the safe harbor accords, and we update that almost on a daily basis.

Mr. HORN. Mr. Belair, is there a negative effect on the future legislation with regard to public records and with respect to the Freedom of Information Act among others and the Electronic Freedom of Information Act? And we asked that yesterday, and I'm just curious if any of you have feelings on that, but we'll start at this end.

Mr. BELAIR. I do. I think the public records debate, which, as you know, the Vice President announced a couple of summers ago that he was going to lead, is an extraordinarily important public discussion. Personal information is available in public record repositories for a reason, public safety reasons, reasons that have to do with the operation of governmental agencies, the fairness involved in giving individuals who have availed themselves of governmental resources for a license for some other kind of a benefit or a status, letting their fellow citizens see who they are and what kinds of resources they are using.

There are a lot of very important public purposes that are served by access to public records. Now that these records increasingly are automated and are commercially available, we're faced with a decision that we weren't faced with 10 years ago, and that is do we really mean that we want this information to be fully and effectively and conveniently public. The answer is—surely isn't to throw it out and close down the records as we started to do with motor vehicle information. The answer is the kind of balance we've been talking about on this panel, figuring out, and I would hope your Commission—I hope the Commission would tackle this—figuring out what are the public values served by the access and what kinds of privacy threats are incurred and then striking a balance.

Mr. HORN. Dr. Culnan, you agree with that statement?

Ms. CULNAN. In part. I think the public record issue is one of the really difficult ones that merits an expansive public conversation. The Internet has really changed the way public records are now accessible to anyone for any purpose. I worked on the Drivers Privacy Protection Act, Mr. Moran's bill, in the House and testified at the Judiciary hearings on that bill before it was passed.

I think the issue that concerns people is not that their information is used for the purpose for which it was provided, to drive a car, to register a car, to get a license to be in a profession, or to fish or whatever, it's that the information is available to anybody for any purpose, and in privacy, a distinction is made between compatible and incompatible uses of information or between the reason the information was collected versus secondary uses, and I think the issue is how do you make the information available for the purposes for which it was collected, be they public service or public safety or other types of important reasons and not allow them to be used for marketing and people looking up other people's information out of curiosity, which really has nothing to do with why the information was collected, and which is the source of the privacy concerns.

Mr. HORN. Ms. Varney, do you agree with that?

Ms. VARNEY. I agree with Dr. Culnan, but I'd modify her last point where she said not allow the information to be used for other purposes. I would say not allow the information to be used for other purposes without consent.

Ms. CULNAN. I would modify my statement to agree with that. Choice.

Mr. HORN. Explain that a little more, because you talk pretty fast, so let's slow it down and tell us what is your real wording here.

Ms. VARNEY. My real wording is I do agree with what Dr. Culnan said as she has now modified it. The balance between the use of the information for purposes that it was provided and intended to be used for and other uses, and I don't think that we want to put a blanket prohibition on other uses. I think we need to look at what are the other uses and what is the correct level of choice that an individual needs to be able to exercise over what may be called unrelated or incompatible uses.

When you go—I don't know if you ever used this example, Mary, but when you go and get your driver's license, and you're 5-foot–4, and you put your weight in, and all of a sudden if you weigh

a fair amount, you may be getting mailers from the Large and Heavy Dress Shop. That's not why I gave my weight information for the Drivers Protection Act. However, I might consent to the use of information if I'm 4-foot–10 because I like to get catalogues for petite clothes. They are hard to find.

So I think what you have to do, Mr. Chairman, is continue to weigh in this debate what are the reasonable expectations of the consumer, what are the economic benefits, and what are the economic costs, and where do you—where can you empower consumers to make their own choices and where can't you. And the where can't you is where law needs to come in.

Mr. HORN. Your dilemma would make a good Cathy strip.

Ms. Singleton, what would you add to this?

Ms. SINGLETON. I'd question again the idea that marketing uses should be presumed to be illegitimate. I think you have a lot of existing businesses that are currently using public records as a part of making goods and services available to consumers, and it's particularly important for companies offering financial services. Risk assessment is a large part of their business, and they need information to do that effectively.

What I would suggest is an alternative approach to the public records problem, which is to focus on it as a security issue, and that is to figure out ways to make sure that the information can be in the hands of legitimate users whether it's a business, trying to sell a product, or somebody looking for their lost child or something like that, and yet keep it out of the hands of people who will use it to do really serious harm, such as stalkers and so on.

Mr. HORN. Mr. Plesser, how about you?

Mr. PLESSER. I think I would go back to agreeing with Mr. Belair, and just to reinforce that, I think there are public record systems whose very purpose of collection is disclosure. Real estate records have been collected by counties in the United States since the beginning of government for the purpose of disclosing ownership and who owns what, and it's been very critical in the Midwest and other areas. People are concerned about false ownership or use of nominees and all of that stuff, environmental issues.

I don't think we can question each use. Where the system of records was collected for the purpose of disclosure with UCC filings, real estate filings, things like that, I think it is critical to have those remain open to the public. If they are now more efficiently distributed, then that's the society that we live in. I think to restrict them to say that you can only use—only licensed real estate agents can get real estate records would really be a travesty and would really potentially start to allow for some of the record control issues that we don't like. And one of the reasons why we've rejected the European system is because we don't want that kind of oppressive government control. And if government records are not open, even ones that have individual records, I think it would really threaten the concept of the freedom of information that you, Mr. Horn, have been very effective in the last number of years in protecting in electronic format, and I would urge you to continue to do that.

Mr. HORN. Mr. Sokul, last response to this question, and then we'll escalate to 12-minute rounds.

Mr. SOKUL. I just have a brief comment. My concern is more along the lines—goes more toward the collection of new information and in particular for tax purposes. I think that privacy is going to be the sleeping giant and probably the ultimate Achilles heel of what the States want to do in the Internet tax arena. There is also a balance that comes into play in terms of invasiveness and intrusiveness and what the country will count for its tax collection.

Mr. HORN. I thank you all for answering that question. It will be very helpful to us in a report to the full committee.

I now yield 13 minutes to the gentleman from Texas Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. I want to revisit this subject of the comp decision of the Commission. I have cosponsored this bill because I feel that we have an issue on our hands that is of such importance and is changing so rapidly that the American people need to have discourse and dialog about it. And this Commission is one way to generate that kind of discussion, but I do think it's important to think about who would serve on this Commission.

I noticed, Ms. Singleton, in your statement you said that we should write specific membership requirements into the bill in order to avoid what you call the usual suspects with an agenda as Commission members. I might ask you to tell us what you meant when you said that the usual suspects, and then perhaps offer to us the type of individuals that perhaps should serve on this Commission. You seem to emphasize the importance of fact-finding, even suggesting that perhaps the members of the Commission should not suggest policy or make policy suggestions, but rather be more fact-finders. I think there had been uniform agreement—I saw the heads nodding a minute ago—17 might be too many, but if we're going to have a discussion like this, we need all the stakeholders at the table.

Perhaps we could start with you, Ms. Singleton, and respond to my question and then offer your suggestions on what the Commission should look like, what type of individuals, what background, and then I'll ask all the rest of you, and maybe we can get a nice long list of the type of people who need to be at the table.

Ms. SINGLETON. I don't have some of the same experiences that some of my fellow panelists do with actually being on a commission. Let me try to clarify, first of all, what I said in my written statement.

I think the emphasis of the Commission should be rather than replicating a lot of the testimony that has already been generated in privacy debates and privacy legislation, should be to focus on things that are unknowns, that there's very little information about already. And I think in particular it would be very beneficial to have a lot of hard economic information there about, for example, the way small businesses use information, the way nonprofits use information, that kind of information. And so I think from my standpoint, it would be very important to have one or two economists represented on the Commission; I mean actual full-bore professional economists, not lawyers who have clerked for judges who were economists.

Perhaps when I talk about the usual suspects on the panel, I'm excluding myself more than anything because I'm not an economist.

Mr. TURNER. You're talking about lawyers as the usual suspects?

Ms. SINGLETON. That would be me, yeah.

Mr. TURNER. One or two economists. So obviously the collection of the economic data you're talking about could be done by staff, but you think we need someone with a background in economics to be able to interpret it?

Ms. SINGLETON. Yes. I think that would be very helpful. I think it's unreasonable that the Commission itself would actually do the economic study. I think it would be more likely that they would contract out with an independent firm that does that kind of thing as a matter of course.

Mr. TURNER. Let me just go down the panel because I'd like to have your suggestions on what kind of individual, what background an individual should have, what training and also to think in terms of the broad range of individuals that should be heard from if we expect to have a full dialog on this issue. Let's start with Mr. Belair.

Mr. BELAIR. I think you're wise to go back to it. I think it's a key issue, and it's a hard issue. I could probably answer it better in terms of who shouldn't be on there.

I had the experience of being the reporter for the National Conference of Commissioners on Uniform State Laws on their health information privacy bill, and they pride themselves on bringing to the table smart people who know nothing about the area, who come at it absolutely clean. I can tell you that that didn't work in the privacy area, and it seems to me with an 18-month run here and a huge agenda, it won't work.

I've also had the experience recently of chairing an effort to bring together experts on criminal justice privacy, and we brought folks to the table with real agendas, real stakeholders. The discussion was terrific, but we ended up of necessity having to make the recommendations very generic and very vanilla because we simply couldn't reach a consensus otherwise.

I guess I wouldn't bring to the Commission table folks who come really locked into a particular agenda or point of view because then you're obligated to bring in their opposite numbers, and there's no way you're ever going to get any kind of a consensus.

I think probably Solveig has got the right idea, bring people who have got some understanding and background with privacy with particular areas of expertise, economics, law, and we can all think of some other areas that would be important to have there.

Ms. CULNAN. I would agree that in the interest of getting the Commission up and running quickly, it's important to have people who are familiar with the privacy issue and have thought about it and been involved in some of the previous discussions about this. I think you should strive to bring people in who are independent and open-minded to the extent that they can be, and I would also argue in favor of selecting people that represent different areas of subject expertise. And in particular somebody with a technology background would be very important because the technology is changing so quickly. It would probably be useful to have someone who understands the law, but you don't necessarily have to have a lawyer.

Ms. VARNEY. I would agree entirely. Seven to nine Commissioners who are viewed as independent and not beholding to any particular commercial or advocacy interest, with particular subject matter expertise in economics, technology, law, finance, and health information.

Mr. PLESSER. I brought with me a relic, which is the report of the Privacy Protection Study Commission that we issued in 1977, and I looked at the front page, and it occurred to me that it might be helpful for this conversation for me to just give you a quick rundown of what the backgrounds of the members of the Commission back then were, because I think it really did—whatever people say of the Privacy Commission, I think it worked. People got together, they got along, and I think there was consensus.

David Linowes was the chairman of the Commission. He was a very experienced CPA, brought to the discussion a lot of expertise and that was very important. He was also a professor and a businessman.

Dr. Willis Ware, who was vicechair, was mentioned before, was probably the leading technologist at the time. He was an expert for Moran Corp. and was considered, I think, the leading computer scientist in the United States at the time. Certainly I would say what Christine said about the importance of having really a world-class technologist. He was that.

William O. Bailey was the president of Aetna, major businessman, CEO, major responsibilities, who did spend a week a month or—the requirement.

Then we had Barry Goldwater, Jr., and Ed Koch, two Congressmen who were very committed to the issue, and I see my friend Ed Markey behind me, and the parallels remind me. But the issue of having two Congressmen actually were effective. They really brought a real sense of reality and realism. I'm not suggesting that that necessarily be done, but I think they were very effective members.

And there was Robert Hennason, and this is an important category. He was a State Senator, and so we had the input, and he had actually worked on Minnesota privacy code, so we had the experience of somebody who really had worked with and understood State problems.

And then finally we had William Dickinson, who was a retired editor of the Philadelphia Inquirer, and it was critical, I think very helpful, to have somebody with that kind of a free press, open communication background.

So there was a balance in here from kind of professions and general point of views. There was nobody, with the exception of maybe Mr. Bailey, that you could say was an industry rep or an anti-industry rep. Everybody else brought to it, I think, a balance of professions, and I would suggest that the idea of having a technologist, a journalist, an accountant, those are all very important aspects.

Mr. TURNER. Do you recall, Mr. Plesser, when the statute that created that Commission in 1977, did they specify the type of individuals that should serve, or did it just work out?

Mr. PLESSER. I don't think so. It specified that three from the executive branch, two from the House, and two from the Senate. I don't recall if it required a specific qualification of specific members

like Stan's committee. I think it did say that there should be a balance of interests, and I think people—there was really no controversy, and I can tell you that this group functioned extremely well. There was really no—there was disagreement on policy issues, but it really was a group, including Mr. Bailey at the time, who was kind of a business representative, really worked hard to do the right thing.

Mr. TURNER. Mr. Sokul, what's your suggestions on membership?

Mr. SOKUL. Our Commission had 19 members, and that was unwieldy. I remember the first meeting the whole morning was just opening statements. But I think——

Mr. HORN. I might say that's a disease that also happens in the Congress.

Mr. SOKUL. I think that with your appointment process, when you're having different people appoint different—a certain number of appointments, it's going to be hard—unless you legislate an individual person in, you're always going to be rolling the dice. It's going to be very difficult to obtain the balance or the perfection you want.

I think the most important thing or the two most important things are that the people are committed and that they talk to each other. I think the Members here probably understand that. I think our best meeting was our final meeting where it wasn't a formalized structure, but Governor Gilmore just adjourned the meeting, and we were in recess in the back room, finally talking to each other.

Maybe the best thing you could do is to exempt the Commission for a few working meetings from the Sunshine Act and just let them go off in private and talk to each other.

Mr. TURNER. You think the Commission ought to have a little privacy, I gather.

I think all your suggestions have been helpful. I guess the next question is open, is whether there should be some specification of these types of individuals in the legislation, or in the alternative, should there be some prohibition against, say, an industry representative or some other type of individual from being able to serve. Do any of you have any suggestions or thoughts on that point?

Ms. SINGLETON. I'll start, since it seems like nobody else is going to. What I'll say is contrary to what some people have said about avoiding extremes. I think part of the reason that the debate has been polarized is that there are real philosophical differences there, and I think it would be to some extent a shame if the Commission did not reflect to some extent those real philosophical differences. And at the same time I think it's still possible to have a commission that avoids fractiousness by—simply by choosing people with certain personality types to be on the Commission as opposed to people who are given to pounding the table with their shoes and so on. That may be easier said than done, of course, but I think—I don't think it would make sense to exclusively prohibit any particular perspective from being expressed.

I won't say any more than that. I think probably others have more expertise about whether it would be more effective to list or not to list.

Mr. BELAIR. As I listened to the discussion, I think I was convinced that certain kinds of subject matter expertise are absolutely vital, technology, some kind of background in finance, economics, and we spelled out several others. I think I'd be tempted, if I were writing the bill, to spell that out a little bit and maybe also allow for some flexibility as well in the appointment process. But it seemed to me that I was convinced that there ought to be some of those kinds of people at the Commission table.

Mr. PLESSER. I just think that while it's very important to think about the Commission members and positions, I think it's very important that we make sure that the inquiry is a full and balanced one if we do do it. The Privacy Commission had something like 60 days of hearings, had hundreds of witnesses, and I think that that process really—I mean, if somebody had a point of view, it would be very difficult to kind of just stay on it. There was a public record and testimony and balanced input.

I certainly agree that you shouldn't have all businesspeople. You shouldn't all have all public interest people. You shouldn't have all academics. There has to be some balance, and I think hopefully the process of appointment will do that, and I think you can say that appointments should reflect a range of—I think at least I would like to avoid saying there has to be one member who represents this interest, one member who represents that interest. I think that would probably not be good. It also would not be good if there were nine CEOs of Web companies on there and nobody else. That would not be a good result, nor would it be good to have nine public privacy advocates on it.

So we have to work to get a process. I think the difficulty is we don't want it to be like slots. We want good people, balanced people representing a range of perspectives, at least that's my view.

Ms. CULNAN. I'll just add very quickly I think it's important to have flexibility. You may get a person that is representing more than one type of expertise, and so, again, by specifying one person, one form of expertise, I think that's a mistake.

I think it would also be a mistake to specify that certain types of people are not to be appointed, to be as general as possible to maintain flexibility to get the very best set of people that you can get.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. I thank the gentleman.

I now yield to the gentleman from Arkansas, Mr. Hutchison.

Mr. HUTCHINSON. Thank you, Mr. Chairman, and this has been a long session, and then we've got another panel, but just to further elaborate on the record somewhat, I did want to ask Mr. Plesser some followup questions about the 1974 Privacy Study Commission. You had some very positive comments to make concerning that. Would you describe what the benefits were of that Commission and what good came out of it from a congressional standpoint?

Mr. PLESSER. There was only one piece of legislation that I think could be directly pointed. There were 164 recommendations for some kind of legislative implementation. There was only really one statute, the Right to Financial Privacy Act, that I think resulted directly from the work of the Commission. During the work of the

Commission, the IRS statute in terms of limiting the information that could be exchanged or given to the executive branch was put in, but I think that would have happened probably with or without us. I think the Right to Financial Privacy Act was a direct result of what we did, which protected people's interests in their checking accounts and information that banks can disclose.

We recommended strongly regulation in the medical records area. It isn't really until this year, 23 years later, that we're seeing legislation in the medical area. My own view is that it was much delayed, but I think even though Bob Belair did kind of a subsequent inquiry into it, I think that the work we did in medical records and employment and specific areas made a great contribution, and I think it's still used today in many areas in analyzing privacy.

Mr. HUTCHINSON. Let me just add when I look at a commission, you never know what's going to happen down the road, but I think information is invaluable to Congress, and actually I think that the argument for the supermajority is that it makes some requirement for consensus to be built, but we also want—the consideration is that if you have a simple majority, you will have a report that comes out and a minority report, and it's information, different viewpoints. The legislative processes still have to work, but it's a tool to build consensus in this very difficult area.

And so I look back to the 1974 Commission. You're right, legislation did result from it in not all of the arenas, but the other information, someone referenced that it's still being passed around today and studied today and referred to today. So I see a lot of benefits from a Member of Congress's standpoint to having this type of commission.

There was—one more question with regard to that. Everybody's talked about the variety of people on the Commission. Is there anything special about the 1974 Commission as to who did the appointing process and who we should be looking at? You've seen our bill, and we have it divided among different congressional leaders and the executive branch.

Mr. PLESSER. Well, the political—I forget exactly the politics back then, but I think you had one party controlling the House, Senate, and President and executive branch, so there wasn't any real political controversy, and in that case you had two from the Senate, two from the House, and three from the administration, but the administration could name the Chair. So that was—I think by having the ability of the administration to do the Chair, they had a little edge, but—if you do a party split. So that's the way that worked. Whether or not it's the best way—it did work in practice. It was, as I said, a balanced approach, but who knows what could have happened.

Did I respond to your question?

Mr. HUTCHINSON. Yes, you did. I'm grateful for that.

Did anyone raise the objection during that time about, well, why do we want to have a commission? We just need to pass legislation right now. We know what we need to do.

Mr. PLESSER. Let me tell you, even though it was slightly before my time, and I might say not only was the Commission balanced, but I think the staff was balanced. Carol Parsons, who was an ex-

tremely able executive director, and she had a privacy background, and she was the executive director of the very early HHS study on privacy, which really developed this concept of fair information practices, and I was a freedom of information lawyer. And so they had a privacy person and an open government, open access person, and I think there was a reason for having that balance, so I think that was effective.

Mr. HUTCHINSON. Were you leading to the question I just asked, though?

Mr. PLESSER. Sure. Could you repeat it? I interrupted. I'm sorry.

Mr. HUTCHINSON. You're still on the other question, trying to give a more complete answer. I was simply asking at that time did people raise the objection that we don't need to have a commission, we ought to just move forward with substantive legislation now.

Mr. PLESSER. What happened at that time was in 1974, the Privacy Act was sponsored by Senator Ervin, and some version recommended the omnibus approach for State and Federal—State, Federal, and private sector records. The Privacy Act, some earlier version was going to cover everything. There was a split. There were a lot of people who did not want that to happen, at least in terms of the private sector and State and local government.

The compromise was the Commission. The compromise was to say, OK, we'll pass the Privacy Act of 1974 in connection with Federal records, but then we will throw this issue of whether or not the principles of the Privacy Act should be extended to private sector and State and local to the Commission. The context was a little different. I mean, they started with a comprehensive law. I think here now the context is somewhat different.

Mr. BELAIR. I was at the White House Privacy Committee at the time, and I think Ron is exactly right. There was a wide consensus that we needed to sort out whether the standards that would apply to Federal Government in the Privacy Act should be applied to the private sector, but there was also a push back in some areas. For example, health privacy even back then was a major concern, and as we got later on into the 1970's, Senator Javits had a bill. There were bills over here—Bella Abzug had a number of bills—and there was a concern that the Privacy Commission's work would slow down the march toward comprehensive health information privacy legislation. As we've seen with hindsight, there were so many things slowing down that legislation, that the Privacy Commission made no contribution to that.

Let me just say real briefly, though, I think Ron's being modest a bit about the work of the Privacy Protection Study Commission. It set the template. It set the model for not just the U.S. thinking, but the whole world's thinking for many, many years about privacy, fair information practices, a distinction between uses of information that had an impact, a tangible impact, on individuals and nonadministrative uses that did not, a sector-by-sector approach, which the Europeans eventually abandoned, but not right away. It had an absolutely, I think, profound impact on the way in which the Nation thought about privacy.

Mr. HUTCHINSON. Thank you.

Mr. HORN. I thank the gentleman, and I yield to the gentleman from Virginia, who I believe will yield to the gentleman from Mas-

sachusetts, who is welcome to bring up himself to the podium here, or you can grab one of the mics. Let me make a deal to you and your two colleagues that disappeared. If you want to be the lead witnesses at 2 p.m., on Thursday, we'd be glad to give you that.

Mr. MARKEY. Thank you, Mr. Chairman, but I think I would rather be the last witness on this panel.

Mr. MORAN. Do we have a choice as to whether you get the last word?

Mr. MARKEY. You just chose, and I thank you so much.

Ms. VARNEY. Mr. Chairman, I have a child care conflict. Could I be excused and give Mr. Markey my seat?

Mr. HORN. Certainly. If you don't mind, we're going to close it down really after Mr. Markey, but we'd like to send you a few questions. Would you mind responding to us for the record?

Ms. CULNAN. I'd be glad to.

Mr. HORN. The gentleman from Massachusetts.

Mr. MORAN. We appreciate very much Ms. Varney coming to testify. Thank you, Christine. If you want to get in the middle here, you can.

The rest of the panel is going to stay because I know they want to hear from you. I'm not going to ask questions. I can review the testimony, but I've also got a prize constituent in Mr. Belair, and I consult with him regularly, so I will take advantage of that. So the floor is all yours.

STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Mr. MARKEY. I thank you very much for your hospitality. Here's my bottom-line point to you all. Members of Congress are experts on privacy. Our privacy isn't invaded on an ongoing basis. You don't have to be—there's a lot of things on which congressional expert is an oxymoron, but compared to real experts, we're really not. But on privacy, we're experts.

The reason that we are experts is for the most part that we're human beings, and that's why we've been able to pass laws over the last several years to deal with issues as they arose that dealt with the privacy of Americans. For example, if someone wants to divulge your driver's license, it's opt-in; all that information, opt-in. That's a law. If someone wants to transfer information about your videocassette rentals, all those things that Judge Bork got in trouble for during this confirmation hearing, Congress passed a law. They can't sell that information to anybody anymore. Opt-in. You want people to know every movie you rented? Opt-in. Pretty simple. What protection would you want for your family? How complicated is that?

How about the information dealing with whether or not the cable company should be able to sell all the information where you click on your cable stations, especially after midnight when everyone is upstairs asleep, what channels you go to; should that be public information everyone has access to? We have a law in the country that says opt-in. Unless you want the cable company to sell that information to people, no one knows what channels you click to when everyone is upstairs asleep. Good law.

How about your tax returns? Opt-in. Do we really have to be experts? Do we have to have a panel put together to decide whether or not we want our tax returns given out to everybody in town, everybody should have access to it? Opt-in. Very simple.

How about on your cell phone when you travel someplace, you might not want everyone to know where you are going? How about the cell phone companies selling that information where you've been going? Opt-in. How about all your phone records, everyone you're calling all day long, everyone in your family is calling all day long? Should anyone be able to access that? Opt-in. Very simple. Not complicated.

We don't need an expert panel on this subject, and we definitely don't need an expert panel to study for 18 months. That is absolutely beyond the pale.

Two years ago when there was a bill coming through to ban pornography on-line, I said, fine, I'll go along with that, but how about giving me an On-Line Child Privacy Protection Act, too; any child 13 and under, unless their parent gives permission, has all that information private. That's the law of the Nation now. The Federal Trade Commission has promulgated the rule. How complicated is that, information for 13 and under should not be disclosed even if you got it on-line, even though it might impede the new Internet revolution?

How about a child who's 13, 14, or 15, though. Do we need a panel to discuss that one, 18 months for us all to figure it out? I don't think so.

How about—how about our health records? How about the fact that your husband or wife has prostate cancer or breast cancer, or a child is on Ritalin or has a child psychiatrist? Should all the medical exams in the insurance company be able to be shared with all the stockbrokers that are in that same firm? How about all the checks that you wrote; all the medical information is on there. Do we need 18 months to figure this out?

I think we need a panel of 17 Members of Congress to go into a room, just give everyone the questions, and everyone will decide, because this is an issue that ultimately deals with your family.

Now, I think the biggest fear that everybody has, to be honest with you, is whether or not any decisions we make are going to affect the Internet and will be responsible for the destruction of the Internet. We shouldn't actually value the Internet the same way we value all companies, because if we valued the Internet the way we value all companies, they'd have to have earnings. They'd actually have to have profits. God forbid we should actually have that standard. People who talk about that lead to the NASDAQ collapsing 2,000 points. How can we possibly have that standard? Obviously we shouldn't have—otherwise everyone who's responsible for saying that they should have profits or earnings or revenues are ruining the new era.

How about fraud on-line or gambling on-line or selling drugs on-line; do we need a study on these issues before we pass any laws with regard to these things that are done on the Internet? Why should we allow, then, for people to be able to delay another 2 years? And that's what we're talking about right here, sitting right here 2 years from now after an 18-month study, which finally goes

to the President later on this year, is finally promulgated, and we're not going to move on anything because there's a chorus here that is going to go out there as soon as this becomes law saying, we've got to wait for Congress now, we've got to wait for the expert panel. God forbid we should decide.

The test here is whether or not we can construct a formula. Commerce, yes, but commerce with a conscience. And the issue, the way I see it, in this bill, by the way, is that, yeah, they are going to look at how the government goes into your business, but I really don't see the private sector—where is the subpoena power for private corporations so you can look at them or the right to depose private corporations? Because the issue, ladies and gentlemen, is not Big Brother, it's Big Browser. The problem is that you can now profile for profits. You can take each one of us, each one of our families, gather information from all these various sources that are now available, put it in a big package, and then sell it to hundreds of companies or others that want to look at our families.

Now, I don't know why we want to study this for 2 more years because we already know it's right on videocassettes, and we know it's right on taxes, and we know its right on cell phones, we know it's right on telephones, we know it's right on everything, ladies and gentlemen. It's very simple.

So my bottom line on this is that this is a basic human right, the right to be let alone, the right for the world not to become—coming into our living room. Wall Street says, we're going to give you a window on Wall Street. That's great. But the American people just don't want Wall Street to have a window in our living room. If we don't want them in our living room, they don't have any right to come into our living room, and if we want to opt in to get all this great information that they want to give us, we can just check off someplace.

By the way, these same companies that say, oh, it's going to be so difficult for us to construct an electronic way in which people can check off they don't want privacy, these are the same companies that tell us they can transfer $1 trillion from here to Osaka in a nanosecond, that they can recreate entire economies in China over the next 2 or 3 years if we are allowed to sell telecommunications and Internet and software technologies into that country, but we can't think, figure out in our own country whether or not we want to protect children, whether or not we want to protect health records? I don't think so.

So this is without question, with all due respect, to all the members of this panel, a central—maybe the central civil rights issue of the 21st century. Eighteen months is too long. This bill really is not going to give the proper authority, be able to look at what the private sector is doing. The Commission is totally tilted. You can wind up, if George Bush is President, with 4 Democrats and 13 Members of the other party are appointed by him, with industry representatives dictating ultimately what they believe is best for their business.

So at the end of the day, we have to have the new economy, but the new economy with old values, and the old values of the very same ones we grew up with, the nurse and the doctor that probed our medical records, and no one else in town knows what happened

to us or member of our family; the banker who gave us our little passbook when we went in for the first time, and no one in the rest of the town is going to know what is in our little passbook, and we know who he is and is going to protect us. Same values.

These companies are going to make it, but they are going to make it protecting against the compromise of our privacy by engaging in other behavior which we all know is wrong. If they are going to be profitable, they are going to have to do it the old-fashioned way, protecting solid American values while using new technology to drive the old companies out of business, but not using new values to drive the old companies out of business. They should be forced to compete on the same grounds in terms of the values.

So I thank you, Mr. Chairman, for allowing me to testify. This is a very important bill, and I think ultimately, with all due respect to the gentleman from Arkansas who I respect very much, I just think it delays too long congressional consideration of this very important issue. Thank you.

Mr. HORN. I thank the gentleman for coming.

I wonder what you would think of the delay that we've had between the Senate and the House. We wanted to get to this in this committee 3 years ago, and everybody was going off in 20 different ways around here, and I just wonder what you think about that if we'd done the Commission 3 or 4 years ago.

Mr. MARKEY. Again, we don't need a commission.

Mr. HORN. But somewhere you need people building a consensus.

Mr. MARKEY. The consensus will be built. Eighty-five percent of all Americans have the same view on this issue. There's a consensus in America already. There's just no consensus when you fill up the room with a bunch of lobbyists, a bunch of industry representatives. Of course they are all no, no, no. If you want to weight them equally with the 85 percent of the American people who agree on every one of these health care, financial records, child—go down the line—disclosure of privacy, there's no debate in America. You can have a technical debate over how to do it, but there's no debate on this question.

This is the single highest polling issue in America. People value their privacy, their individuality, their American—their sense of independence of the big business and big government. The far left and the libertarian right join on this issue, doesn't leave a lot of room in the middle. They are fighting this hard, Mr. Barton and I, Senator Shelby and Senator Bryan in the Senate. It's the middle, the practical middle—actually it's the business middle that objects.

So, yeah, we can pass this, but we pass it only for big business, only for big bucks, only for Big Browser, but we're not passing it for ordinary people. That's not what this study is about, because every one of us know what protection we want for our mothers, for our fathers, our wives, our husbands, for our children. Every one of us know what that answer is on every single subject. We're all experts on that.

Mr. HORN. Before you leave, I'll call on the author and coauthor of the bill and see if you want to ask any questions of the gentleman from Massachusetts. Mr. Moran still has plenty of time.

Mr. MORAN. But we don't have much time here. I've got to get to a meeting with Mr. Gephardt that started at 4:15, so I can't get into too much questioning.

We have heard from many people who are not tied into a commercial entity, nor have a commercial motivation, who feel that this is a more complex issue than it appears to be, and certainly than you perceive it to be, Mr. Markey. There are a number of different State approaches, some of them conflicting. We have legislation that was passed with regard to medical privacy that HHS has gotten tens of thousands of responses on and has taken 2 or 3 years to try to come up with some regulations. We have the financial services modernization bill that was recently passed that is legislation. I know you opposed it, but nevertheless—opposed at least parts of it. I think you voted against the bill, as I recall, but nevertheless was passed and is the law of the land and has a significant implication for the—for the privacy issue in general, and there will be others.

And one of the purposes of such a commission was to try to establish some consistency, some fundamental principles, some floor, if you will, when you talk about values, some value floor that would either exempt or incorporate or preempt, I should say, or incorporate State law. I don't think that we want a potpourri of different State statutes. Clearly electronic commerce is intrastate, can't be held within boundaries, and we have a difficult issue with regard to preemption or finding some kind of consistent uniformity.

We also have a difficult issue, if we're going to ad hoc this kind of legislation, whether it be in financial services or medical issues or other types of electronic commerce, how we achieve consistency, and we also have very rapid developments in the field itself and the industry, developments that are customer-friendly, developments that respond to market incentives.

People want privacy. We don't disagree that this is a cutting-edge issue. If you poll them using any kind of simplistic question, you're going to get very high responses. People want privacy. And so the industries involved in the Internet and information technology understand that and have responded with any number of ways to protect people's privacy.

And so the intent of giving the Congress some analysis with which to develop overarching legislation, if you will, was to achieve consistency, was to recognize the central tenets of federalism, and was to incorporate technological advances that have been taking place in the private sector, and also to figure out a way that we can coordinate the public and the private sector, because we don't necessarily have the parallel objectives here. There are some benefits to the public sector having some information shared that the private sector collects.

So for all those reasons, there seem to be some benefit to studying the issue, and, as Mr. Horn said, no matter how anxious many Members might be to get legislation enacted immediately, it is not likely to happen. The history is that it has held up for what seems to be interminable periods—certainly longer than 18 months. If you look at financial services, we've been working on that for what, 10 years. Medical privacy took a significant amount of time to get legislated, but even more time to get regulated. So you could make an

argument that if we could get a consistent format and some consensus within 18 months, we'd be doing pretty well, and even breaking some precedent.

Do you want to respond to those? I see you've been taking some notes there.

Mr. MARKEY. I agree with you that each individual in America should be able to avail themselves of the new privacy technologies, encryption technologies that are being developed. That's important. They also have basically a right to expect industry to voluntarily step forward and put together industry standards, and they are in some fields, some companies. But because there are always going to be a significant number of outliers, significant number of companies on-line, especially who are just digital desperadoes, just trying to capture whatever they can in a short period of time in this new economy, there has to be a Federal floor. There has to be a third level of Federal guarantee, a right to knowledge that information is being gathered about you, a right to know that it's going to be reused for purposes other than you and your family intended it, and third a right to say no. And then you've got some power, too, even if the technology doesn't work to block it, even if the companies aren't going to be doing it. You've got a right as an American, a right to protect your own family's secrets, secrets you are not telling anyone else about.

In Europe they have stronger standards, and from Citicorp to every American company that is over there, they abide by these stronger privacy codes, and our industry is thriving in Europe, abiding by the tougher European privacy codes.

Many people say, we don't want the European standards here in America, but when you poll in America, 85 percent of Americans say they want the European standards. Now, we didn't import 500 people for this poll. They are all Americans. They are just ordinary people. They want the same standards. And the reason that we didn't build in the right for an American to stop the transfer of their medical insurance records in an insurance company now to a broker or banking affiliate is that the Rules Committee last year wouldn't allow my amendment out on the floor because they knew it was going to pass 350–50. That's the only reason it didn't pass. I couldn't get it made in order. The industry said, don't allow that amendment, because they had won in the Commerce Committee 42–0. No Member wanted to vote against it when they were forced to in the Commerce Committee that they would have their medical or financial information transferred without their permission, so they just blocked the vote on the floor. Didn't need any more study. Every Member knew they didn't want their family's medical privacy spread around town or those checks or those insurance exams. It was the industry using the Rules Committee.

So, yeah, I guess you can say we can bottle everything up, use the process to stop it, but I don't think it's an accurate reflection of the amount of knowledge that we all have of what it is that we want to be built into law for each of our families. And all I'm doing is just reflecting my own mother's mortification if someone knew of some illness that she had. She wouldn't even tell her sisters, much less everyone in town, if she was—if she had an incontinence pad. She wouldn't want anyone to know that.

She should have a right to protect that. Every American should have that right. I don't think we need to debate it. I don't think we need to wait 2 more years for this industry to have the same rules that the old industries have. I think we owe that to Americans, and waiting 2 more years means waiting 4 more years.

Mr. MORAN. I was just going to suggest that this may seem like a plodding, tedious process to bring everybody together at the same table and to try to reach some consensus, but sometimes the plodding, tedious process actually accomplishes more in terms of legislative enactment than the dance of legislation, which can be more thrilling and seemingly responsive, but can oftentimes take longer and can become even more frustrating.

Mr. MARKEY. I'll tell you what happened. In the 1995 Telecommunications Act, our privacy bill of rights was built into that act, and it was worked out by all the Democrats and Republicans on the Commerce Committee, and it passed the House, and you voted for it. Every Member here voted for it in 1995. It was my bill. I worked it out with Jack Fields, I worked it out with all the Republicans, and it was a comprehensive privacy on-line bill of rights.

The reason it got knocked out was not that all the Members didn't understand what the language was, it was because the Republican leadership, a week before we finished the conference in February 1996, just knocked it out, just knocked it out. Somebody called them, and they just knocked it out. And I was in the minority at that point, so I didn't have any power to keep it back in, but it was all worked out in a bipartisan, bicameral, industry-inclusive basis. That was 5 years ago now, 6 years ago.

So we can study it, I guess, until 10 years has elapsed since the anniversary of the 1995 act passed on the floor of the House, but I just don't think we all need to know much more about this subject.

Mr. MORAN. Well, you make a very persuasive presentation as always, Mr. Markey.

Mr. MARKEY. It's the Jesuit education.

Mr. MORAN. I was going to make a remark about that, but you beat me to the punch.

Mr. HORN. I thought it was just being Irish.

The gentleman from Arkansas.

Mr. HUTCHINSON. Thank you, Mr. Chairman.

Being a visitor to your subcommittee, I want to tell you how impressed I am with the depth of your hearings. This has been extraordinarily a mind-expanding experience, and I want to thank the gentleman from Massachusetts Mr. Markey for his excellent presentation. I think that added certainly to the debate today.

And I've been thinking about that we had a discussion early on, and if we take this bill, Mr. Moran and I, we just took this bill totally down and say we want to give it every shot, we don't want to give anybody an excuse not to support industry privacy legislation, in all honesty I don't think it's going to—you'll build the consensus to move it forward this year. In all honesty I don't think you've got the timeframe to get it done this year.

That's just my view, but I don't want this again to be used as an excuse not to move other legislation through. I see it complementary. In some areas I think you can—we can all agree upon

the more simple, basic, fundamental areas of privacy, if we need to do something, let's do it and get it done with.

I asked this from the White House yesterday, the gentleman from the Office of Management and Budget, if you adopt these other things you're interested in, would it be some benefit to a commission looking at the ongoing technology, the ongoing privacy issues? His answer was yes, because it's a changing world out there. This issue is not—adopt everything that you want to adopt, Mr. Markey, everything that you want to adopt, and I still believe that we need a commission to look at the ongoing developing issues in a comprehensive fashion. So that's really my interest in it.

And then maybe—you raise these illustrations about opt-in, and I—quite frankly, I don't know if it is that simple. There was an instance the other day if there was an opt-in where someone refused to give a consent for information to be transferred, an opt-in for a cell phone company, what if a person chooses not to opt in and they call from a cell phone with an emergency, but the location of that emergency cannot be divulged to law enforcement or the fire department? Now, it could be a kidnapping, it could be a rape circumstance. And actually this information was shared a few weeks ago when a lady was kidnapped and she called the police, and the telephone company did not want to share the information.

There very well is an answer to that, appropriate exception, but I think the point is that this is—there's some areas there that we need to—that should be debated, discussed. It is not as simplistic as sometimes is presented on the front end.

And so I hope we'll continue having this discussion, and I want to thank you again, Mr. Markey, for your presentation. You're making notes. I'll give you a chance to respond.

Mr. MARKEY. I thank you so much. On that specific issue which you just raised, in fact, we passed a bill that does prohibit the tracking of cell phone use, but with an emergency exception, so in that particular instance, there was no reason why the company could not transfer the information to the police or the fire in order to provide rescue or emergency medical service for that individual. As a matter of fact, we passed a specific law a year ago in order to accomplish that goal.

And on the other issue, again, I'm just reflecting my own personal history, which is that the Rules Committee 3 years ago, when we were bringing up the financial services bill, it ultimately was a failed effort. They would not permit my amendment on privacy to be put in order for the floor, but they promised there would be comprehensive hearings. That was the Banking Committee promise. There were no hearings. And last year in 1999, when my amendment was denied consideration on the House floor, they promised hearings this year. There have been no hearings. So if we want to now conduct a study for 2 more years, I think it passes prologue. We already see in the conduct of——

Mr. HUTCHINSON. Mr. Markey, you mentioned 2 years a couple of times. I do want to emphasize because of that point, there's a provision that the Commission can report back early if they deem it appropriate. If there's a consensus that develops within 2 months, they report back to Congress. And so that is an outside

sunset time, and excuse me for interrupting, but I did want to make that point.

Mr. MARKEY. With $2.5 million allocated, we're going to invoke the rule that work expands the time allotted without question, because the salaries of all these staffers that are going to be hired and all the expert witnesses will guarantee that they'll go right up to the very last minute.

Mr. HUTCHINSON. There was a comment. Mr. Plesser, you raised your hand a moment ago.

Mr. WAXMAN. Are we doing the 5-minute rule?

Mr. HORN. We went to the 13-minute rule, and we'll be glad to give you the same.

Mr. PLESSER. If I can, and I appreciate all the comments that Congressman Markey said. I just want to say that I think his review of the statutes in saying opt-in simply reflect it's somewhat more complex than that. I know he would agree with it, although the legislation that he suggested does have some affirmative consent proceedings in it, but it also has opt-out in terms of the use of mailing lists, marketing lists, not of the specifics of the transaction. But many of the statutes that he referred to, the Cable Act and others, other of the statutes do provide provisions, both a balanced view of opt-out and opt-in. Mr. Markey has always had this wonderful concept of notice, knowledge and no, which I think has really led the industry and has led self-regulatory efforts, and I think we just want to make sure that it still is notice, knowledge and no, and not opt-in under some circumstances.

I would certainly agree in medical records and in detail the kind of examples that he gave, but I think opt-out also has a strong role, and I just wanted to just fulfill the record on that point.

Mr. MARKEY. If I could just followup on that, I agree with him, a lot of the medical and financial information is very sensitive and should be given opt-in protection. And a lot of the other information that's on-line is more prosaic and probably doesn't deserve opt-in. But we don't need a year and a half to figure out which is and which isn't. We can definitely finish the medical and financial that we know should be given that protection. The most important issue is the material that deals with the financial and health information. We don't need to wait another 18 months. If you want, we can have a commission on what should be the rules for the prosaic information, but I don't think we need more time on that.

Mr. HUTCHINSON. Mr. Chairman, I yield back. Thank you.

Mr. HORN. The gentleman from California Mr. Waxman, 10 minutes.

Mr. WAXMAN. Thank you, Mr. Chairman, for the time. I had a conflict and couldn't be here. I thought the House rules provided for 5 minutes. I wondered after 5 minutes had gone by and no clock evidently keeping track of things of what the rules were. I won't take 10 minutes, but I wanted a chance to at least ask a few questions.

Mr. Markey, I can see you're frustrated. I'm frustrated because we tried to do something in the area of medical privacy together, and the legislation has been introduced. Other people have introduced bills on medical privacy. This committee, which has jurisdiction, hasn't even held a hearing on medical privacy. We'll probably

have a commission to review the findings of the Commission, and then we have to wonder when are we going to get to the point where we're going to do something about it, because I think the American people are concerned.

In the area of medical privacy, individuals have expressed concern that their employers or potential employers will have an inappropriate access to personal information about their health records, and I recently conducted a survey to investigate how large employers handle their employees' health records. I asked 48 top Fortune 500 companies to voluntarily describe their privacy practices regarding handling of their employees' health information and to voluntarily provide documentation of their privacy policies.

While a few companies stood out for having quality components to their policies, the survey found that only 15 of the 48 companies provided documentation of company policies on medical privacy, and many of the policies provided—lacked critical details. Further, 11 of the 48 companies refused to respond to any of the survey questions.

So I think it's fair to ask if companies are unwilling to share information with Congress, why would they be any more willing to volunteer information to a congressionally appointed Privacy Commission?

Mr. Markey, you have been deeply involved in medical privacy policy. If we do go forward with establishing a Privacy Commission, do you think we should require the Commission to examine employer practices and policies with respect to health information of their employees, and do you think the Commission should be given the power to secure information from companies regarding such practices and policies?

Mr. MARKEY. I do. I think that there should be a power of subpoena, there should be a right to depose, without question. We're talking about the most fundamental civil rights that we each have, which is the right to keep our own medical secrets private. It's no one else's business. And if companies are out there engaging in practices which compromise that, then I think this committee—the Commission, as it's constructed, and as a result the American people, should know this, and as a result then the legislation which is formulated subsequent to that would reflect the protections that have to be built in against those practices.

Mr. WAXMAN. Another area which many individuals have expressed concern is how financial institutions handle personal information. The United Kingdom has recently established a public registry that helps individuals learn about what types of personal data is being maintained and used by data collectors, meaning entities that decide how and why personal data are processed. Under UK law, data controllers have to provide details to the public, register about how they process personal information. The registers can be searched on-line by entering the name of the particular data controller. The register includes a description of the different purposes for which the controller holds or uses personal data, describes the types of personal data held or maintained.

I want to share with you the results of a recent staff search on this registry for Citibank International. The stated purposes for which the personal data is held or used include marketing and sell-

ing, including direct marketing to individuals, personnel/employee administration and business and technological intelligence, among many others. For each purpose listed, the registry described the types of personal data held or used. As an example, I'd like to turn to the category marketing and selling including direct marketing to individuals, and listed 46 different categories of information including personal details, physical descriptions, habits, personality, character, current marriage or partnership, marital history, details of other family household members, other social contacts, immigration status, leisure activities interests, lifestyle, academic record, court tribunal inquiry proceedings, liabilities, outgoings, loans, mortgages, credits, dietary and other special health requirements, and religious beliefs. Obviously the register established in the United Kingdom provides individuals with a tool for obtaining substantial information about the practices of data controllers.

Mr. Markey, you've worked for many years on financial privacy policy. Do you think it would be a good use of resources to study whether an information register like the one established in the United Kingdom would be a valuable system to establish in the United States, and if we move forward with legislation to establish a Privacy Commission, do you think the bill should require the Commission to review the United Kingdom's public register system and make recommendations regarding establishing a similar system in the United States? And do you think the Commission should have the power to secure information from companies relevant to this study?

Mr. MARKEY. I do. What you're now describing is something that was required from the World Wide Web consortium, and the British, as a result, were saying to Citicorp, you've got to tell us what you're using this information for, give us your white paper, tell us what's in there. So you just basically listed a financial services FBI file on an individual gathered by Citicorp on these Europeans. And Citicorp was very unhappy about that, that it was disclosed to the public, because they might get the jitters that that kind of detailed profile on them is being gathered.

Now, there's one thing we can be sure of, that Citicorp is doing the same thing to all of its customers in America, except we don't know about it because we don't have law the way they have over there, this data protection registry in Great Britain. And once the public understood it, they obviously were outraged. So we need a way in which the public and the United States knows about what Citicorp and every other corporation is doing in terms of this information, and if we don't do that, then we're going to ultimately wind up with all of us having this—you know, this digital dossier being developed on us and our families that tells those companies more about ourselves than any member of our own family know about us as individuals.

So you put your finger right on it, Mr. Waxman. There's the core problem, and I think we could have corrected it in the financial services bill last year. I think we can correct it this year. We had a week of hearings now. We can all agree on what should be done. I don't think we have to wait 18 months.

Mr. WAXMAN. Do any of the members of the panel think we ought to have this Commission with the power to get this informa-

tion from employers as to what they do on medical privacy and be hired to study the system in the UK and how they are handling these data controllers? Anybody on the panel want to talk to those issues?

Mr. BELAIR. Let me speak to the situation in Europe. I think it's tempting to look across the Atlantic and see a very robust privacy environment. I spent a lot of time in Europe this year. I know Ron has, and I'm sure others have as well. Of course, a number of the EU nations have not yet implemented their own national law. In addition, the EU is suing some of those nations for their failure to comply, and what's fascinating about the European situation, it took a while to figure that out, but as you talk to the American, the United States affiliates over there or multinational corporations, there's such a different enforcement culture there that, in fact, I think it's fair to say, and indeed many Europeans say, that there is a very liberal interpretation of both the EU directive and the national laws. And so I think one——

Mr. WAXMAN. What is your conclusion? You don't think we ought to study it because it's too different?

Mr. BELAIR. No, I think it bears study, but I don't think it is necessarily a model for us. I do believe, and I think probably——

Mr. WAXMAN. We don't know that until we study it.

Do you think a commission ought to be able to study this and ought to be looking at other models?

Mr. BELAIR. No question about it. Absolutely. I said that in my testimony.

Mr. WAXMAN. How about some of the others? If you want to talk about the medical privacy issue, if employers are not willing to respond to Congress on what their policies are, do we need to give a subpoena power to this Commission to get the information?

Ms. CULNAN. I would say there's clearly a need for better notice in this country. I'm not sure that a registration system run by the government is the way to do it, but I think clearly that the Commission certainly could look at comparative models and see what could work here and what wouldn't. But it's particularly important, as Mr. Markey said, that people be informed what information organizations hold on them, and what's the most effective way to do that I think is the real issue.

I think in terms of collecting information from companies, I think it would be important to assure them anonymity. To me, I don't think there's any particular benefit in naming names and saying one company does this and one company does that, but it would be very important to get a sense of the landscape in terms of where the problems are, as I said in my testimony, the extent to which fair information practices are applied, and that would include do employees know what companies are doing with their information.

Mr. WAXMAN. I see my time is up. I don't know if the chairman wants to allow anybody else to speak on this issue.

Mr. HORN. Once you ask the question, the Horn rule is to let everybody else answer, but that's it. Then we move to the next person.

Mr. Greenwood is with us.

Who else would like to answer——

Mr. WAXMAN. Anybody. I just wanted to know if anybody wanted to respond. I didn't ask each one to respond.

Ms. SINGLETON. Just a very quick comment. I understand Germany also looked at the possibility of a central registry and rejected the possibility because they were concerned it could become a target for human rights violations to have a list somewhere of all the information and immediately somebody who you don't want to have access to that list get access to it. It becomes a tool in the wrong hands.

With respect to the subpoena power, I second Professor Culnan's remarks on the anonymity. I think it would be very valuable to get a picture of how information is actually used in the economy, particularly in the form of a survey, and that anonymity would help to ensure great participation.

Mr. PLESSER. On the subpoena power question, yes, no question, the Privacy Commission had it in the mid-1970's. It was horrible and unwieldy to use, and I don't think we ever used it, but the threat of it was effective. Without it I don't think anybody would have spoken to us.

Whether or not you go forward with a commission, I think broader subpoena power is a good idea. I don't think there should be any limit on what you want to study. I think if you want to study data registration in Europe, that's fine. There has been one issue of which there is total unanimity among every person who has looked at privacy in the United States. Every privacy advocate, every expert, everybody that I've known or ever spoke to have always opposed the concept of data registration being imported to the United States. I've never heard even the most radical privacy advocate ask for that.

I think it's important to study it, to consider it. I think in the end the comment we just heard that it's really anti-privacy rather than pro-privacy is appropriate because then the officials know where to go, then they know how to organize it and have the map. I think the problem of data registration is a significant one, and it's antithetical to our tradition and never really has been seriously suggested for the United States. But absolutely, let's have a study, let's look at it and see if there's a way that some of those concepts are helpful, but also to find out what the negative concepts would be. Thank you.

Mr. HORN. Mr. Sokul, any comment to Mr. Waxman's question?

Thank you very much.

We now have Mr. Greenwood, Jim Greenwood from the State of Pennsylvania.

Mr. HUTCHINSON. Mr. Chairman, are the panelists that have been here, are they expected to stay?

Mr. HORN. Well, we'd certainly welcome them, but the dialog with the Members—I think Mr. Waxman's question deserved an answer, and we went down the line, but you're certainly free to leave, and we will, as I said earlier, send you some questions, if you don't mind. We're going to ask Democratic counsel and Republican counsel what key questions did we miss, and we'd appreciate your writing us back. We'll put it at this point in the record without objection.

So we now turn to Mr. Greenwood, and we're delighted to have him here. He had to suffer the long wait that you and Mr. Markey and Mr. Barton gave up, I gather, and you're always welcome. You're a real leader in the House, and we're glad to have you here.

Mr. GREENWOOD. Thank you, Mr. Chairman. I will be brief because, unfortunately, my schedule is going to require that as well.

You've been listening to testimony for 3 hours on this issue, so I'm not sure how much more enlightenment I can offer. But I would like to share with you why it is that I am prime sponsor of H.R. 2470, which is the Medical Information Protection and Research Enhancement Act, which is an attempt to legislate this issue this year, and I'm also a sponsor of Mr. Hutchison's bill, H.R. 4049, the Privacy Commission Act bill, which you've been hearing of.

As you know, this is a long-standing and highly controversial issue and a very important issue. Back in 1996, the Congress basically directed and passed HIPAA, that required, if we couldn't get our act together legislatively by the summer of last year, that HCFA would do the regulations. We couldn't. We failed as a Congress to legislate. During that 3-year interim, I introduced my bill in July of last year, and we've not been able to move it, and there are reasons for that.

This is like any other controversy. This issue involves the collision of a couple of values: of course, the commitment that we all have to protect privacy with regard to the most intimate details of our lives. The second one is that there's a terrific benefit to society when medical outcomes can be—that data can be collected and can be used by researchers and health care providers and insurers and others to try to enhance therapies and treatments for all of us. So the challenge in this issue is how do you merge these two values without compromising, on the one hand, confidentiality, nor compromising, on the other hand, the ability of society to benefit from this data.

My experience with this issue is that there are two fundamental policy roadblocks, the first of those has to do with liability. The consumer advocates generally represented by the Democrats in the House advocate for a relatively liberal policy with regard to liability. They believe that if one's confidentiality is breached in any way, that there ought to be ready access to the courts.

The other issue of controversy has to do with preemption. Many of us, including myself, perceive that in this digital age, information travels from our health care provider, to our health insurer, to a researcher across the State lines at the speed of light, and if we are going to use the values of the information age, we need to make sure that this data doesn't have to stop at every State boundary on the way. It won't work that way. The States have moved ahead and have, in some cases, passed some very strict confidentiality laws as it relates to issues like AIDS, mental health, and genetic information.

I believe that we need to find a way to build a very airtight channel for this information to move from State to State without violating confidentiality. We haven't been able to do that. I've worked with Congressman Waxman, Congressman Markey, Congressman Brown, and Congresswoman Eshoo on the Commerce Committee

trying to forge bipartisan support for the bill, and frankly we just haven't succeeded. We just haven't been able—in good faith negotiations to reach consensus.

So my first wish would be that my legislation could pass, and we could have it enacted in this Congress. I don't see that, frankly, as being likely. So my second priority would be that Mr. Hutchinson's bill becomes enacted so that we can find, through the use of a commission, the consensus that we've not been able to find legislatively. In my view, the worst of all possible scenarios is that nothing happens, and that this issue drags on for failure on our part to find bipartisan consensus.

Mr. HORN. Does the gentleman from Arkansas have any questions of the witness?

Mr. HUTCHINSON. No. I just want to thank you for putting a good cap on this hearing today. You expressed really what my attitude is. I'd like to see your legislation move forward first and foremost, and I appreciate your understanding that this commission bill—I don't want it to be a threat to anyone's individual bill. I want to it to be complementary, I want it to be helpful and take a long-term look.

So thank you very much for expressing that so succinctly and for your support and your initiative, which I'm delighted to support, and also for your support of the Commission.

So thank you, Mr. Greenwood.

Mr. GREENWOOD. If Mr. Horn would take my bill up and move it, I would be happy to have it transfered to this committee.

Mr. HORN. It's sitting in the Commerce Committee. Can you get it over here? We'll give you a fast 24-hour look at it.

We have to vote on the floor, and I want to thank the staff that helped prepare this hearing. We will hold another hearing tomorrow, which I believe will be Thursday—yes, Thursday at 2, and it will be on privacy. I guess we haven't learned enough yet.

And we want to thank the court reporter Laurie Harris. I don't know how you stood it, Laurie. You should have nodded, I guess.

And the staff director and Chief Counsel George has been with us in and out. Heather Bailey is to my left, your right, as the professional staff member putting things together here; and Bonnie Heald, director of communication; Bryan Sisk, clerk; Liz Seong, intern; and Michael Soon, intern. Trey Henderson is counsel for the minority, and Jean Gosa is minority clerk. And with that, we adjourn the meeting.

[Whereupon, at 5:06 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

TESTIMONY OF REPRESENTATIVE EDWARD J. MARKEY (D-MA)
BEFORE THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
GOVERNMENT REFORM COMMITTEE
MAY 16, 2000

Mr. Chairman and Members of the Subcommittee, thank you for allowing me to testify before you on this very important issue.

Privacy. The right to be let alone. One of the most basic values of our society – an old value threatened by a new economy. The question of the hour is how to protect this value that we all hold sacred? How to animate our new economy with our old values. How to create commerce with a conscience.

In the old economy the issue of privacy triggered thoughts of George Orwell's *1984* and Big Brother government driven by its hunger for control over its citizenry. In 2000, the threat to privacy has evolved to Big Browser driven by private industry's hunger for big bucks.

Right now, when it comes to your financial records, there are very few protections against a financial services firm from disclosing every check you've ever written, every credit card charge you've ever made, the medical exam you got before you received health insurance. And as you surf the Web, there are no rules in place to prevent various web sites from collecting information about what sites you are viewing and how long you are viewing them. If you buy anything over the Internet, that information can be linked up to other personal identifiers to create a disturbingly detailed digital dossier that can profile your lifestyle, your interests, your hobbies, or your habits. The name of the game is Profiling for Profits and in this game we all lose –we lose our right to keep our personal information private.

The Privacy Commission bill seeks to address the fact that we have moved to an information-based economy. In its findings, the bill states that in "light of recent changes in financial services laws," there is a need for a coordinated and comprehensive review "of the protections of personal data compiled by the health care, insurance, and financial services industries."

Indeed with the passage of last year's banking bill the barriers between banks, insurers and securities firms have crumbled allowing for the free flow of information between these newly created affiliates. The Gramm-Leach-Bliley Act provided very weak privacy protections to consumers, giving them the right to "opt out" of having their personal, nonpublic financial information transferred to unaffiliated third parties. However, there are no limits on disclosures to affiliates. Furthermore, there's a "joint marketing agreement" provision that allows disclosures of a customer's information to nonaffiliated third parties with which the institution has signed a contract. These two loopholes render the limited "opt out" requirements in the bill a pathetic joke. And last week, we learned that the financial regulators have decided to delay full implementation of even these minimal privacy protections until July 2001.

We need to do more now. A Commission that takes 18 months with the broad mission of comprehensively studying privacy practices will do nothing to provide consumers with the protections they need right away. And although I know this bill is not intended to impede legislative action, I am concerned that those who oppose privacy protections will use the Commission as an excuse to delay effective federal privacy protections.

Under current law, we have an "opt-in" for a tax preparer transferring your tax return to any other party. We have an opt-in before drivers license information can be transferred. We

have an opt-in for information about videocassette rentals. We have an opt-in for cable TV viewing habits. We have an opt-in for telephone call records. We have an opt-in for information about cell phone whereabouts. But we do not have an opt-in for sensitive financial information and for certain medical information.

So you see, Mr. Chairman, the threat to privacy is a real-time issue and with each passing day, as more and more mergers take place, more and more of your personal information will be sloshed between affiliates of large financial holding companies. We have no time to waste with respect to curbing the free flow of information that currently exists. We need to act now, we need to protect the personal information of Americans today. A Commission sounds like a step in the right direction but the effect will be to paralyze legislative action for 18 months. Furthermore, those of us who have been active on privacy are ready with solutions today.

Representative Joe Barton (R-TX) and I have been focused on privacy for quite some time now – together we co-chair the Bipartisan, Bicameral Congressional Caucus on Privacy, we have organized over 28 Congressional Members with the common goal of providing Americans with the strongest federal privacy protections as soon as possible. Caucus members support and agree that the following four basic principles should be included in any federal privacy proposal:

- Americans should have a right to clear and conspicuous notice of how their information will be used, for what purpose and to whom it will be disclosed;
- Americans should have the right to give their prior affirmative consent before a private company or governmental agency uses and/or discloses that individual's information for any purpose other than that for which it was originally given;
- Americans deserve a right to access and correct any personally identifiable information held by a private company or governmental agency;
- and finally, with respect to preemption, the Caucus agrees that individuals should benefit from the strongest privacy protections available -- therefore, federal privacy protections must not preempt state laws or other regulations that provide stronger privacy protections.

Together Rep. Barton and I have introduced H.R. 3320, the "Consumer's Right to Financial Privacy Act," which would close the affiliate sharing and joint marketing loopholes and require an "opt in" before a financial institution could disclose sensitive financial information. Our bill currently has 71 bipartisan cosponsors, including Ranking Member Waxman and 7 other Members of the Government Reform Committee. The companion bill in the Senate has been introduced by Senators Richard Shelby (R-AL) and Richard Bryan (D-NV). In addition, I have also joined with Representatives John LaFalce (D-NY) and John Dingell (D-MI) in introducing the Administration's privacy proposal, H.R. 4380, which would establish an "opt in" for medical information and sensitive information about a consumer's spending habits, and an "opt out" for the disclosure of other nonpublic personal information about the consumer.

I have also introduced legislation to address medical privacy and internet privacy H.R. 1057, The Medical Information Privacy and Security Act and H.R. 3321, the Electronic Privacy Bill of Rights.

So you see, Mr. Chairmen, there are already good proposals waiting for action. I urge you to join us in taking action in protecting the privacy of Americans today and reconsider moving forward with the Commission at this time.

I thank you.

STATEMENT OF
CONGRESSMAN JAMES P. MORAN. JR.
BEFORE THE SUBCOMMITTEE
ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
HEARING ON HUTCHINSON/MORAN PRIVACY COMMISSION ACT

May 15, 2000

CHAIRMAN HORN, MEMBERS OF THE SUBCOMMITTEE, Thank you for the opportunity to appear before you with Congressman Hutchinson for this hearing on H.R. 4049, the Privacy Commission Act.

Americans are more and more aware and concerned that their personal information is not as secure as they would like. In fact, in a Wall Street Journal/NBC News poll last fall, loss of personal privacy ranked in the top list of issues that concern Americans in the new century.

These 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. 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, there are no uniform standards ensuring individuals' protections.

At the same time we must recognize that the United States is the leading economic and social force in the global economy, largely because of a favorable regulatory climate and the free flow of information and there is a danger of over-reaction in privacy regulation.

The U.S. Internet economy is already worth an estimated $350 billion. 72 million American adults, some 35 percent of the American population, are expected to be on-line by the end of this year. 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 that what is needed is a thoughtful, deliberate approach to privacy issues by Congress.

This 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 in Congress to examine the threats to the privacy of Americans and to report back on what legislation may be necessary.

It also directs the Commission to report on non-legislative solutions. If self-regulation can be improved, how should industry achieve it? 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.

In short, this is a balanced, measured approach to a complex issue. I commend Mr. Hutchinson for his leadership on it and I commend this committee for holding hearings on this subject.

Statement of the Honorable Jim Turner
GMIT Legislative Hearing: H.R. 4049, "To Establish the Commission for Comprehensive Study of Privacy Protection"
May 15, 2000

Thank you, Mr. Chairman. This is the second of three hearings that we have scheduled on H.R. 4049, and I commend the Chairman for prioritizing the need to study this important issue. Without a doubt, privacy is one of the top concerns of the American people and one of the most important issues facing this Congress. Therefore, I was pleased to become a cosponsor of this legislation which would create a commission that will enable us to have a full and open discussion with the American people about privacy so that we can address it in an appropriate manner. However, I do not want us to rush forward with this bill without preceding cautiously and carefully considering the number of issues surrounding the creation of this Commission.

In our first hearing, witnesses raised questions regarding the relationship the Commission's work would have with privacy efforts by other entities. Specifically, concerns were voiced as to whether the Commission could serve as a delay to regulations and studies that are currently moving forward. For example, witnesses pointed out that a bipartisan congressional privacy caucus is currently pressing for passage of a financial privacy measure. Pursuant to a congressional mandate, the Secretary of HHS is now in the process of finalizing medical privacy regulations. Additionally, the Department of Treasury's study on financial privacy regulations is soon to be completed. We have many privacy issues that need to be dealt with immediately, and I was pleased to hear Congressman Hutchinson state that the intent of the bill was not to impede the progress of other legislation or

regulations that we may achieve consensus on during the existence of the Commission. Rather, it would be used as a sounding board to those initiatives.

Moreover, questions have arisen regarding the composition and expertise of members selected to the Commission. Currently, the bill does not contain requirements regarding the qualifications of Commission members. We need to ensure that an appropriate balance between all stakeholders in this issue are represented. Witnesses also questioned the scope of the Commission's mandate, which currently is not limited as set forth in the bill. We should be concerned about duplicating work that has already been done and consider whether it might be more productive for the Commission to focus on specific privacy issues.

In light of the concerns that witnesses raised at the first hearing, members of past and present entities charged with studying privacy issues, as well as federal and state government representatives who have been active on privacy matters, have been asked to testify before the Subcommittee. These witnesses are expected to address the types of expertise and background that should be sought in Commission members, the types of issues that should receive focus by the Commission, and the types of reviews that may be redundant.

Again, I commend the Chairman for holding these hearings and welcome the witnesses hear today. Mr. Waxman also appreciates your scheduling these hearings to help ensure that the issues raised by H.R. 4049 receive careful consideration. Mr. Waxman regrets that he is unable to attend today's hearing due to a previous commitment, but he plans to attend tomorrow's hearing and looks forward to reviewing the testimony from today's hearing. The American people

deserve to have their privacy protected in a correct, judicious, and timely manner. It is my hope that as a result of these hearings we will be closer to this goal.

AMERICAN SOCIETY OF NEWSPAPER EDITORS

ADDRESS: 11690B Sunrise Valley Drive, Reston VA 20191-1409 • PHONE: 703/453-1122
FAX: 703/453-1133 • E-MAIL: asne@asne.org • WEB: http://www.asne.org

Richard A. Oppel
Austin (Texas)
American-Statesman
President

Tim J. McGuire
Star Tribune, Minneapolis
Vice President

Diane H. McFarlin
Sarasota (Fla.)
Herald-Tribune
Secretary

Peter K. Bhatia
The Oregonian, Portland
Treasurer

The Board of Directors consists of the officers and the following:

N. Christian Anderson III
The Orange County Register,
Santa Ana, Calif.

Richard Aregood
The Star-Ledger,
Newark, N.J.

Gilbert Bailon
The Dallas Morning News

Jennie Buckner
The Charlotte
(N.C.) Observer

Kenneth F. Bunting
Seattle Post-Intelligencer

Susan C. Deans
Denver Rocky
Mountain News

Frank M. Denton
Wisconsin State Journal,
Madison

Karla Garrett Harshaw
Springfield
(Ohio) News-Sun

Pamela J. Johnson
The Arizona Republic, Phoenix

Edward W. Jones
The Free Lance-Star,
Fredericksburg, Va.

Wanda S. Lloyd
The Greenville (S.C.) News

Robert G. McGruder
Detroit Free Press

Gregory L. Moore
The Boston Globe

Rick Rodriguez
The Sacramento (Calif.) Bee

Paul C. Tash
St. Petersburg (Fla.) Times

David A. Zeeck
The News Tribune,
Tacoma, Wash.

June 28, 2000

The Honorable Dan Burton
Chairman
Committee on Government Reform
United States House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Dear Rep. Burton:

The American Society of Newspaper Editors, the nation's largest organization of newspaper editors, understands the depth of concerns about invasions of individual privacy. We also see clearly the value of open records and protection of the First Amendment.

Clearly, with the advent particularly of the Internet, we have a troubling and confusing situation that needs careful, prudent sorting out. It is in the public's interest for a thorough and fair examination of privacy issues to be carried out by a balanced, thoughtful panel.

In that spirit, we support enactment H.R. 4049, "The Privacy Commission Act."

Going forward, ASNE offers to assist in any way possible with the proposed commission to assure a fair resolution of privacy issues.

Thank you for your consideration.

Sincerely,

Richard A. Oppel

cc: Hon. Henry Waxman

[For Staff Director George & Ms Bailey - in hearing record?]

PRIVACY TIMES

5/27/2000

The Honorable Steve Horn
Chairman
House Committee on Government Reform
Subcommittee On Government Management
U.S. House of Representatives
House Rayburn Office Building
Washington, D.C. 20515

May 22, 2000

Dear Congressman Horn:

Thank you for the invitation to submit our collective comments on HR 4049, a bill to create a Privacy Study Commission.

No matter how well-intentioned, we oppose this bill because it is unlikely to advance privacy protection in the United States. To the contrary, if adopted, it would likely retard the progress of legislation that would result in meaningful legal protections for Americans.

There are several reasons to oppose this bill, many of which have been cited by Rep. Ed Markey (D-MA) and Robert Gellman, a privacy consultant, in testimony before your subcommittee.

First, as a practical matter, it will delay Congressional consideration of much-needed privacy legislation. If a study commission were created, many Members of Congress would adopt the view that it "would be premature to consider privacy legislation until the study commission finishes its work." Indeed, Congressman Henry Waxman cited an editorial from one industry publication exhorting industry to support the measure because it *would* delay consideration of real privacy legislation. Protecting Americans' privacy is much too urgent to build-in the kinds of structural delays that a study commission would entail.

Second, we are concerned that the proposed study commission would be stacked with representatives from industries that already have publicly opposed legal privacy rights for Americans. Thus, the commission would have no credibility and would be a waste of taxpayer money.

Third, the public record is replete with testimony and evidence of the urgent need for comprehensive privacy legislation. For example, since 1977, when the Privacy Protection Study Commission released its report, there has been broad consensus that the use of personal information should be based upon "Fair Information Practices (FIPs)."

Privacy Times, P.O. Box 21501, Washington, D.C. 20009 • Tel: (202) 829-3660 • Fax: (202) 829-3653

FIPs are the bases for several laws, like the Privacy Act of 1974, the Fair Credit Reporting Act, The Cable Privacy Act, and the Video Rental Privacy, and for the 1980 Guidelines of the Organization of Economic Cooperation & Development (OECD), to which the United States is a signatory. A robust public record, ranging from Congressional hearings to hearings by the Federal Trade Commission, Federal Communications Commission, Commerce Department and others, supports arguments for extending FIPs to all kinds of personal information. This can only be done by legislation.

Fourth, and most importantly, the American public has made it clear through a series opinion surveys that their privacy is not adequately protected, and that they want laws enacted so it is adequately protected. The public response has been consistent and overwhelmingly in favor of privacy legislation, running between 75 and 90 percent. In other words, there is a clear *consensus* among the public that stronger privacy laws are necessary. The only place where there is not consensus on this issue is among some industries (and their Washington lobbyists) that want to continue to exploit consumers' personal data without consumers' consent, and among some government agencies.

Fifth, enacting this bill would give the *appearance* that Congress was finally doing something about protecting Americans' right to privacy, when in fact it wasn't. Such a result would be unfair to the American people.

In sum, privacy already has been "studied to death," in part because of the desire of some large public and private organizations to forestall privacy rights for all Americans. Those Members of Congress who want to advance privacy protection should join the Congressional Privacy Caucus and support legislation already introduced by Members of the Caucus.

Those Members of Congress who consistently decline to advance privacy protection may someday find it difficult to explain why they didn't.

Sincerely Yours,

Evan Hendricks, Editor/Publisher
Privacy Times
Washington, D.C.

David Sobel, General Counsel
Adrew Shen, Political Analyst
Electronic Privacy Information Center
Washington, DC

Ken McEldowney, Executive Director
Consumer Action
San Francisco, CA

Beth Givens, Director
Privacy Rights Clearinghouse
San Diego, CA

Lisa S. Dean,
Free Congress Foundation

Jason Catlett
Junkbusters.com

Mark Budnitz, Chairman of the Board
Consumer Law Center of the South

Stephen Gardner
Attorney At Law
Dallas, Texas

Joanne Faulkner, Attorney At Law
New Haven, CT

Mark Steinbach, Attorney at Law
Washington, DC

Andrew G. Pizor, Attorney at Law
Legal Services Corp. of Delaware, Inc.

David Szwak, Attorney at Law
Shreveport, Louisiana

De Vonna Joy
Consumer Justice Law Center
Muskego, WI

Dale W. Pittman, Attorney at Law
Petersburg, VA

Sharon L. Kinsey, Attorney
Soquel, CA

SALLIE TWENTYMAN
1207 Offutt Drive
Falls Church, VA 22046
(703) 533-7946
April 12, 2000

Honorable Steve Horn
Committee on Government Reform
Subcommittee on Government Management,
Information and Technology
2331 Rayburn House Office Building
Washington, DC 20515-0538

Dear Chairman Horn:

As I told you this morning, I sincerely appreciate the opportunity to testify in this morning's hearing regarding the establishment of the Commission for the Comprehensive Study of Privacy Protection. It was a new experience for me, but an experience that I hope will, in some way, aid in your efforts to preserve the privacy of every American citizen in years to come. It was very clear to me that there is no doubt in each of your minds that a complete review needs to be done, and, for that, I am greatly relieved.

I did wish to add two more points to my testimony and would like my comments herewith to be included into the Subcommittee's official record. I understand your need to stay on schedule and proceed with the second panel, so I decided to send them to you in writing instead of trying to interject them in the proceedings which were already running late:

1-- The task for dealing with identity theft, of course, is two-fold. There are two elements—first, a preventative element with a goal of keeping our personal information out of the hands of criminals, and, second, a curative element which takes action against the perpetrators when a violation unfortunately does occur. It is extremely important that consumer education help American citizens learn to deal with each element—protecting their personal information and understanding what steps to take should they find themselves a victim.

Over the past year, many people have begun to work diligently to increase privacy awareness and educate citizens about what steps to take to decrease their risk of having their personal information stolen. Since becoming a victim myself last summer, my friends and I have seen many stories in the media about identity theft. I was involved in one of these efforts in February of this year, one spearheaded by the U.S. Postal Inspection Service—a video news release which took my story into an estimated 6-8 million households teamed with a training video for law enforcement personnel to help them to know what to do when victims come to them for help.

These educational efforts, both from private and governmental groups, should be commended and encouraged.

2-- One private company which, to me, has been a model company in their information handling policies with me over the past several months is USAA. I have been impressed with the way that they authenticate and verify that the person on the phone is the person whom they claim to be. When I call to make changes to my policies or accounts, they ask me questions regarding the accounts which would be difficult for an impostor to answer—the makes and number of automobiles I have insured, my spouse's name and social security number, what other kinds of accounts I have with them, etc. Other businesses would do well to study their policies and the way they train their employees.

Once again, I want to extend my appreciation of the opportunity to testify this morning. It is a rare privilege to be able to share such experiences so openly with people who have the power to make such a difference. I do wish you the best in your efforts and always stand willing to answer any questions or help you in any way that I can in the future.

Sincerely,

Sallie Twentyman

Sallie Twentyman

Cc: Honorable Jim Turner
Cc: Honorable Asa Hutchinson
Cc: Honorable James P. Moran

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

COMMERCE COMMITTEE
RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS, TRADE
AND CONSUMER PROTECTION
BUDGET COMMITTEE
RESOURCES COMMITTEE
(on leave)

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN BUILDING
WASHINGTON, DC 20515-2107
(202) 225-2836

DISTRICT OFFICES:
5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396-2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875-2900

May 9, 2000

The Honorable Steve Horn, Chairman
Subcommittee on Government Management, Information and Technology
Committee on Government Reform
B-373 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Horn:

We are writing to request an opportunity to testify on Tuesday, May 16th before the Subcommittee on Government Management, Information and Technology with respect to the Privacy Commission Bill.

As co-chairs of the Bipartisan, Bicameral Congressional Caucus on Privacy, we have organized over 28 Congressional Members with the common goal of providing Americans with the strongest federal privacy protections as soon as possible. Caucus members support and agree that the following four basic principles should be included in any federal privacy proposal: First, Americans should have a right to clear and conspicuous notice of how their information will be used, for what purpose and to whom it will be disclosed; second, Americans should have the right to give their prior affirmative consent before a private company or governmental agency uses and/or discloses that individual's information for any purpose other than that for which it was originally given; third, Americans deserve a right to access and correct any personally identifiable information held by a private company or governmental agency; and finally, with respect to preemption, the Caucus agrees that individuals should benefit from the strongest privacy protections available -- therefore, federal privacy protections must not preempt state laws or other regulations that provide stronger privacy protections.

In January, we introduced H.R. 3320, the Consumer's Right to Financial Privacy Act to close the gaping privacy loopholes which exist in the Gramm-Leach-Bliley Act. To date we have 71 co-sponsors signed on to this bill. In addition, Mr. Markey has introduced HR 3321, the Electronic Privacy Bill of Rights, as well as H.R. 1057, the Medical Information Privacy And Security Act.

As privacy has been a primary legislative focus for us, we would appreciate the opportunity to testify at your upcoming hearing on the Privacy Commission Act.

We thank you for your consideration.

Sincerely,

Ed Markey

Joe Barton

cc: The Honorable Jim Turner
The Honorable Henry Waxman

PRINTED ON RECYCLED PAPER

April 26, 2000

The Honorable Stephen Horn
Subcommittee on Government Management, Information and Technology
B-373 Rayburn House Office Building
Washington, D.C. 20515

RE: H.R. 4049 Legislative Hearing Follow-up Questions

Dear Chairman Horn:

Thank you for the opportunity to testify at the April 12, 2000 legislative hearing on H.R. 4049, a bill to establish a commission for privacy protection. I commend the Subcommittee for considering a comprehensive analysis of how to protect the privacy of personal information, without sacrificing the flow of necessary and desirable communications.

I am pleased to respond to the follow-up questions in your April 17, 2000 letter, as outlined below. In addition, please do not hesitate to call on me if I can further assist the subcommittee, or any Commission or Congressional Committee, to learn from Maine's experiences in protecting the confidentiality of health care information.

Please describe the successes and failures of the Maine law.

By way of background, Maine legislators began their careful work on this issue in January 1997. The legislators proceeded cautiously, meeting regularly with all interested parties for over a year. In the spring of 1998, the legislature passed a comprehensive health care privacy law, with an effective date of January 1999. This original law was theoretically sound, and appeared to provide appropriate consumer protections. However, it did not take long for the people of Maine to teach us the critical difference between theoretical principles of personal privacy and their expectations of our health care system. The law was in effect just two weeks before Maine legislators reacted to their constituents' expressions of outrage by suspending it. Notably, it was not the health care providers, civil liberty groups or "official" consumer representatives that complained so bitterly and so relentlessly. The countless, unsolicited, and unorganized complaints to the legislators came from their own constituents. In response, the legislature reconsidered the original law and extensively amended it. Maine's amended health care privacy law has been in effect since February 1, 2000. Both versions of Maine's law to protect the confidentiality of health care information are built on the same legislative foundation. Both versions of Maine law appear to adequately protect personally identifiable health care information. However, a few flaws or "failures" of the Maine law were discovered when we implemented Maine's original law in January 1999, and those were legislatively addressed to become the "successes" in our current amended law.

MHA

The Maine Hospital Association
150 Capitol Street, Augusta, Maine 04330
Tel.: 207/622-4794; Fax: 207/622-3073; Website: www.themha.org

Even Maine's original statute could accurately be described as a "success" in that it declared that personally identifiable health care information was confidential and could not be disclosed by a health care provider, except as provided by law. While this initially may sound like it is stating the obvious, this protective statement had never before been set forth in any prior state or federal law. In addition to heightening awareness of this critical principle, both versions of Maine's law supported that statement of principle with a consistent statewide process for appropriate disclosures, including comprehensive definitions, mandates and prohibitions, to assure that health care information was not inappropriately disclosed. Those protections were carefully balanced against the free exchange of information necessary to provide health care and the consumers' wish to control the disclosures of their health care information. As a result, although the amended law has only been in effect for three months, it appears to be effectively protecting the confidentiality of personally identifiable health care information without blocking the flow of essential and desirable communications.

Nevertheless, we learned some important lessons when we tried to implement our original law in 1999. One of the flaws in the original law was that it restricted the flow of information between health care providers, and between the providers and their patients' families. The law required separate specific written authorizations from the patient for every provider to provider communication outside of the health care provider's office, practice or organization. We found that this requirement could appreciably delay the health care process. This delay was unacceptable, both to the providers and to their patients. The legislators' constituents told them that they *expected* provider to provider communication, to the extent it was necessary to facilitate the provision of their health care. The public also complained about the additional layers of paperwork. The Maine legislature responded by amending the law to state that, in the absence of patient authorization, provider to provider disclosures are generally limited to those made for the purposes of diagnosis, treatment or care of the patient.

Our first law also restricted provider disclosures to family or household members. Without specific written authorization, such disclosures were permitted only if an individual was receiving diagnosis, treatment or care in a health care facility, and then the disclosure was limited to confirming the presence of the individual at the facility and releasing his/her "general health condition." We disagreed with the proponents of that restriction who assured providers that such a restriction would not interfere with health care because the family or friend could tell us everything we needed to know about an incapacitated patient, even though we could tell them very little. Such statutory interference with a provider's communication about their patients impeded health care, particularly if the patient was incapacitated or otherwise unable to provide the necessary authorization. The people of Maine agreed, and strenuously objected to this forced change in long-standing and well-accepted relationships with their providers. Our legislature, therefore, amended the law to allow for provider communication with patients' loved ones, subject to the constraints of professional judgment and ethics. As always, the patient may expressly direct the communication if they are able to do so and wish to do so.

The preceding discussion of Maine law is an excellent illustration of the "opt-in" or "opt-out" debate as mentioned at the April 12 hearing. Maine's original law was drafted as an "opt-in" provision, meaning that the patient needed to expressly choose to authorize the disclosure. Without specific authorization, these disclosures were prohibited. Therefore, if the patient was unable to authorize disclosure to family due to traumatic injuries or temporary incapacity for any other reason, the default process prohibited the disclosures. Maine's amended law reversed this presumption, and allowed more open provider communication with family *unless* the patient expressly directed otherwise, in other words, unless the patient "opted- out." Proponents of Maine's original 1999 version of this section claimed that an ill patient is justifiably concerned with more important issues and should not bear the burden of "opting out. " There was also concern that patients did not fully understand their ability to control the flow of their health care information. While there is undeniably some truth in those statements, we found that restricting that flow of information was unworkable, for the health care providers *and* for their patients. However, the amended law does require that providers give notice to their patients about their ability to control disclosures of their health care information.

Maine's second "failure" was to think that we could comprehensively anticipate every possible appropriate disclosure of protected information. Unfortunately, the unintended consequences of inadvertently restricting appropriate disclosures could be devastating. For example, Maine's first law did not have a specific exception that would permit a relative or friend to refill or pick up a prescription medicine for a home bound loved one. A phone call would not suffice; disclosures of health care information required specific written authorization. And a simple note from the consumer was insufficient, as the statute outlined the elements of a valid authorization. We learned, the hard way, that many people in our state rely on someone else to help them get their prescription medicines quickly. Maine legislators responded to this need by promptly amending the law.

However, Congress or the Department of Health and Human Services could not act so quickly to correct any similar unintended ramifications of a comprehensive federal policy. In fact, the Secretary's proposed rules promise no amendments for at least twelve months.[1] As discussed above, many people could be inadvertently injured by an unforeseen and unintended consequence of regulatory language that must stand for at least a year. Given that the proposed rules contain many provisions proven to be unworkable in our state's experience, we strongly advocate that the Commission review the Secretary's rules before they are finalized. Serious problems could be avoided if a Commission established under H.R. 4049 comprehensively examined these issues, the experiences others have had addressing them, and the need to balance privacy protections against necessary and desirable communications.

Another flaw in Maine's original law was that it required written authorizations, signed by the patient or the patient's legally appointed representative, for disclosures of health care information.

[1] 64 FR 60,050 (1999).

Like so many provisions of the original law, this approach superficially appeared to be a reasonable consumer protection. However, it ultimately proved to be unworkable for two reasons. First, patients complained to their legislators that their verbal authorization ought to be sufficient, particularly if they lived a long distance from the source of the information or were traveling out of state. Consumers believed, and rightly so, that they should be able to direct disclosures and that this control should be available to them without completing additional paperwork. Patients who had moved away or were traveling also complained about the unacceptable delays that occurred because they had to wait for the provider to send out a valid release form to the patient, who may not be someplace where they could receive mail at the time, and then wait until the hospital received the signed form before the requested disclosure would be made to the designated recipient. The Maine legislature responded by further amending the law to allow verbal authorizations if obtaining written authorization was impractical or requested by the patient, and required that providers document such verbal authorization.

A second reason that this section of the original law proved to be unworkable was that there was not a provision allowing a surrogate decision-maker to authorize disclosures of information should the patient be unable to do so, and there was no legally appointed representative. In Maine, we learned that the majority of our patients do not have such legally designated representatives. Our legislature amended the law to allow appropriate surrogate decision-makers to authorize disclosures *if and only if* the patient was unable to do so *and* there was no known legally appointed representative.

Did the Maine legislature base the medical privacy laws on other state statutes?

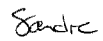
At the time, no other state had statutorily protected the confidentiality of health care information. However, the following list illustrates the resources from other states that were brought forward during the drafting discussions:

- A similar bill defeated in Massachusetts, bill number MA97RHB 1498 filed 12/4/96.
- Consultants from the National Coalition for Patient Rights and the American Civil Liberties Union.
- Massachusetts Medical Society paper titled *Patient Privacy and Confidentiality*, 1996.
- American Medical Association testimony before the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, 1997.
- American Psychiatric Association Resource Document on *Preserving patient Confidentiality in the Era of Information Technology*, 1996.
- American Health Information Management Association testimony in support of the Fair Health Information Practices Act of 1997.
- National Association of Insurance Commissioners Insurance Information and Privacy Protection Model Act.
- Department of Health and Human Services Recommendations to Congress, 1997.
- American Hospital Association Principles for Confidentiality of Health Information.

- American Hospital Association testimony before this Subcommittee on H.R. 52, June 19, 1997.
- American Hospital Association testimony before the Committee on Labor and Human Resources of the United States Senate on the Confidentially of Health Information, October 28, 1997.

Again, thank you very much for the opportunity to share Maine's experiences in legislatively protecting the confidentiality of health care information. I hope that the lessons we learned are helpful, and that any mistakes we may have made, however well intended, are not repeated at the federal level.

Sincerely,



Sandra L. Parker, Esq.
Director, Legal Affairs and Health Policy

cc: Patti Goldman, AHA

MHA

The Maine Hospital Association
150 Capitol Street, Augusta, Maine 04330
Tel.: 207/622-4794; Fax: 207/622-3073; Website: www.themha.org

IDENTICAL LETTERS SENT:

The Honorable Fred Thompson
Chairman
Committee on Government Affairs
United States Senate
Washington, DC 20510

The Honorable David M. Walker
Comptroller General of the United States
General Accounting Office
Washington, DC 20548

The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives
Washington, DC 20515

The Honorable C. W. Bill Young
Chairman
Committee on Appropriations
House of Representatives
Washington, DC 20515

The Honorable Robert C. Byrd
Ranking Minority Member
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Jacob J. Lew
Director
Office of Management and Budget
Washington, DC 20503

The Honorable Joseph Lieberman
Ranking Minority Member
Committee on Government Affairs
United States Senate
Washington, DC 20510

The Honorable David R. Obey
Ranking Minority Member
Committee on Appropriations
House of Representatives
Washington, DC 20515

The Honorable Ted Stevens
Chairman
Committee on Appropriations
United States Senate
Washington, DC 20510

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

The Honorable Stephen Horn
Chairman
Subcommittee on Government Management,
Information and Technology
Committee on Government Reform
U.S. House of Representatives
Washington D.C. 20515

Dear Chairman Horn,

This letter responds to your request for the views of the Department of Justice on H.R. 4049, the "Privacy Commission Act."

The Department strongly supports efforts to safeguard individual privacy. For example, the Attorney General has established a privacy council within the Department of Justice to ensure that privacy issues receive high-level attention and commitment. Moreover, the Department has taken steps to ensure that all Justice Department web sites have accurate privacy policies and we recently completed a comprehensive, Department-wide assessment of our compliance with the Federal Privacy Act.

While we share your concern with the need to protect individual privacy and support efforts to assess the need for stronger privacy safeguards, we are concerned that establishing a privacy commission at this time may have the unintended effect of delaying other privacy legislation that is ripe for congressional action. We do not think that this legislation sufficiently addresses the work to be done in this important area. We look forward to working with you on legislative initiatives such as the following:

- In announcing the draft of the first-ever Federal medical record privacy regulations in October 1999, the President noted that Congress imposed severe limitations on the reach of the privacy regulations and he called on Congress to address these shortcomings in Federal law.

- The President recently issued an Executive Order that bans discrimination in Federal employment on the basis of genetic information and he called on Congress to enact legislation to establish such protections in employment generally.

- The President also has discussed the need for additional safeguards for financial privacy and we anticipate that the Administration will submit financial privacy legislation to Congress in the near future.

We also draw your attention to the extensive initiatives by the Federal government to study and take action in the area of privacy protection. For instance:

- When children go online, parents should give their consent before companies gather personal information. Websites aimed at children must get such consent under the Children's Online Privacy Protection Act of 1998 and rules that go into effect this month.

- The Department of Commerce, the Federal Trade Commission, the Electronic Commerce Working Group, and other parts of the Federal government have undertaken a wide array of studies, reports, workshops, and other activities to address issues of online privacy. Under steady prodding by the Administration, the proportion of commercial websites with privacy policies rose from 15 percent to over 65 percent from 1998 to 1999.

- A public workshop last fall challenged the industry to address concerns about "online profiling," in which companies collect data, in ways few people would suspect, about individuals surfing the Internet.

- The Administration continues to build privacy protections into its own activities. Last year, for instance, all Federal agencies successfully posted clear privacy policies on their websites. Programs are now underway to strengthen Government computer security to provide new privacy safeguards for personal information held by the Government.

With respect to H.R. 4049, we have serious concerns about the membership and mission of the proposed privacy commission. For example, we believe the commission's membership should reflect a more balanced allocation of positions between the Executive and Legislative branches. We question the commission's broad mandate and whether it might be more

productive for the commission to focus on specific privacy issues. We also have concerns about the content and focus of the required report. Again, while we would be happy to work with you on these issues, we would prefer to make progress on other, high priority privacy proposals.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Robert Raben
Assistant Attorney General

IDENTICAL LETTER SENT TO THE HONORABLE JIM TURNER, RANKING MINORITY MEMBER