AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

H.R. 5777, THE "BEST PRACTICES ACT," AND H.R. _____, A DISCUSSION DRAFT TO REQUIRE NOTICE TO AND CONSENT OF AN INDIVIDUAL PRIOR TO THE COLLECTION AND DISCLOSURE OF CERTAIN PERSONAL INFORMATION RELATING TO THAT INDIVIDUAL

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JULY 22, 2010

Serial No. 111–147

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

78–124 WASHINGTON : 2013

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

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
BETTY SUTTON, Ohio
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BOBBY L. RUSH, Illinois
Chairman

JANICE D. SCHAKOWSKY, Illinois
Vice Chair
JOHN SARBANES, Maryland
BETTY SUTTON, Ohio
FRANK PALLONE, JR., NEW JERSEY
BART GORDON, Tennessee
BART STUPAK, Michigan
GENE GREEN, Texas
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
KATHY CASTOR, Florida
ZACHARY T. SPACE, Ohio
BRUCE L. BRALEY, Iowa
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan (ex officio)

CLIFF STEARNS, Florida
Ranking Member
RALPH M. HALL, Texas
ED WHITFIELD, Kentucky
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
MICHAEL C. BURGESS, Texas

CONTENTS

Page

Hon. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement 1
Hon. Ed Whitfield, a Representative in Congress from the Commonwealth of Kentucky, opening statement 85
Prepared statement 87
Hon. Kathy Castor, a Representative in Congress from the State of Florida, opening statement 89
Hon. Steve Scalise, a Representative in Congress from the State of Louisiana, opening statement 89
Hon. Gene Green, a Representative in Congress from the State of Texas, opening statement 90
Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, opening statement 91
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement 95
Hon. Joe Barton, a Representative in Congress from the State of Texas, prepared statement 93

WITNESSES

David Vladeck, Director, Bureau of Consumer Protection, Federal Trade Commission 97
Prepared statement 100
Leslie Harris, President and Chief Executive Officer, Center for Democracy and Technology 123
Prepared statement 125
David Hoffman, Global Privacy Officer, Intel Corporation 137
Prepared statement 139
Ed Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group 149
Prepared statement 151
Ira Rubinstein, Adjunct Professor of Law, New York University School of Law 168
Prepared statement 170
Jason Goldman, Counsel, Technology and E-Commerce, U.S. Chamber of Commerce 180
Prepared statement 182
Mike Zaneis, Vice President, Public Policy, Interactive Advertising Bureau 201
Prepared statement 203

SUBMITTED MATERIAL

H.R. 5777 3
Discussion draft 58

H.R. 5777, THE "BEST PRACTICES ACT," AND H.R. ————, A DISCUSSION DRAFT TO REQUIRE NOTICE TO AND CONSENT OF AN INDIVIDUAL PRIOR TO THE COLLECTION AND DISCLOSURE OF CERTAIN PERSONAL INFORMATION RELATING TO THAT INDIVIDUAL

THURSDAY, JULY 22, 2010

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

The Subcommittee met, pursuant to call, at 2:33 p.m., in Room 2322 of the Rayburn House Office Building, Hon. Bobby L. Rush [Chairman of the Subcommittee] presiding.

Members present: Representatives Rush, Stupak, Green, Barrow, Castor, Space, Boucher, Whitfield, Stearns, Gingrey, Scalise, and Latta.

Staff present: Michelle Ash, Chief Counsel; Timothy Robinson, Counsel; Marc Groman, Counsel; Will Wallace, Special Assistant; Brian McCullough, Senior Professional Staff; Shannon Weinberg, Counsel; Will Carty, Senior Professional Staff and Counselor; Robert Frisby, FTC Detailee; and Sam Costello, Legislative Analyst.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. Good afternoon. Today we are pleased to welcome seven witnesses representing the Federal Trade Commission, the consumers, industry, especially businesses with an Internet presence and whose mainline of business is to create and sell advertising. And I would like to thank them for taking the time out of their busy schedules to share in their perspectives on consumer privacy as well as to outline their view as appropriate offline and online business privacy protection and personal information use practices.

Have you ever been in the midst of a group of people and heard someone say "What is said in this room stays in this room?" As someone in that room you know just from that statement that what may be said could be juicy enough, sensitive enough, or valuable enough to tempt one of the other persons in that room to violate that compact by leaking that information to people who are not in

the room during the discussion. And the very utterance of these words evidences a conscious intent by the participants to set the needed environmental conditions that will encourage those in the room to interact freely with one another to share data, share information without them fearing that that very information will harm them economically, emotionally, or otherwise at some point in the future.

As an avid user of the Internet and as a person interested in technology and communications, and all things visual, I know there is no free lunch when I go onto the Internet and Web site and to read or view content, especially when I am not paying for that content. That Internet Web site and advertisers on the right, and overhead, and operating costs of that Web site know that my information whether it can be used to identify who I am, or whether it gets merged in with other user's information has substantial value and can be monetized when it is provided to others.

Before the House was scheduled to adjourn for its August recess, I for one felt that it was imperative on Monday of this week to introduce privacy legislation in the form of H.R. 5777, the Best Practices Act. I also felt it was important that we quickly hold a hearing in this Subcommittee on the assorted pros and cons of my bill as well as other issues outlined in the discussion draft released by Chairman Boucher and Ranking Member Stearns of the CIT Subcommittee.

The Best Practices Act speaks to a host of issues affecting consumer privacy, including consumer's expectations as to how their personal information should be handled, shared, and disclosed to third parties. This legislation also addresses other important issues including what defaults should be set in connection with those expectations to provide regulatory certainty to industry and to investors. What safeguards should be crafted to anticipate foreseeable abuses and violations of consumer privacy expectations? What sets of remedies will make consumers whole in the event of privacy breach, and how to calibrate penalties and other possible legal causes of action without chilling industry incentives to innovate and grow their businesses.

This legislation also addresses to what extent, if any, should the privacy framework set forth in my bill preempt state privacy laws and regulations. In holding this hearing I would like to get a better handle on how extensively personal information gets shared without an individual's understanding and without their consent. I also want to shine a spotlight on some of the actual harms that befall individual users through no fault of their own.

With that said I yield back the balance of my time.

[H.R. 5777 and the discussion draft follow:]

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

111TH CONGRESS
2D SESSION

H. R. 5777

To foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 19, 2010

Mr. RUSH introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act" or the "BEST PRACTICES Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2 Definitions.

TITLE I—TRANSPARENCY, NOTICE, AND INDIVIDUAL CHOICE

Sec. 101. Information to be made available.
Sec. 102. Provision of notice or notices.
Sec. 103. Opt-out consent required for collection and use of covered information by a covered entity.
Sec. 104. Express affirmative consent.
Sec. 105. Material changes to privacy practices.
Sec. 106. Exceptions.

TITLE II—ACCURACY, ACCESS, AND DISPUTE RESOLUTION

Sec. 201. Accuracy.
Sec. 202. Access and dispute resolution.

TITLE III—DATA SECURITY, DATA MINIMIZATION, AND ACCOUNTABILITY

Sec. 301. Data security.
Sec. 302. Accountability.
Sec. 303. Data minimization obligations.

TITLE IV—SAFE HARBOR AND SELF-REGULATORY CHOICE PROGRAM

Sec. 401. Safe harbor.
Sec. 402. Approval by the Federal Trade Commission.
Sec. 403. Requirements of self-regulatory program.
Sec. 404. Rulemaking.

TITLE V—EXEMPTIONS

Sec. 501. Use of aggregate or deidentified information.
Sec. 502. Activities covered by other Federal privacy laws.

TITLE VI—APPLICATION AND ENFORCEMENT

Sec. 601. General application.
Sec. 602. Enforcement by the Federal Trade Commission.
Sec. 603. Enforcement by State attorneys general.
Sec. 604. Private right of action.
Sec. 605. Effect on other laws.

TITLE VII—MISCELLANEOUS PROVISIONS

Sec. 701. Review.
Sec. 702. Consumer and business education campaign.
Sec. 703. Effective date.
Sec. 704. Severability.

SEC. 2. DEFINITIONS.

As used in this Act, the following definitions apply:

(1) AGGREGATE INFORMATION.—The term "aggregate information" means data that relates to a group or category of services or individuals, from which all information identifying an individual has been removed.

(2) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(3) COVERED ENTITY.—The term "covered entity" means a person engaged in interstate commerce that collects or stores data containing covered information or sensitive information. Such term does not include—

(A) the Federal Government or any instrumentality of the Federal Government, nor the government of any State or political subdivision of a State; or

(B) any person that can demonstrate that such person—

(i) stores covered information from or about fewer than 15,000 individuals;

(ii) collects covered information from or about fewer than 10,000 individuals during any 12-month period;

(iii) does not collect or store sensitive information; and

(iv) does not use covered information to study, monitor, or analyze the behavior of individuals as the person's primary business.

(4) COVERED INFORMATION.—

(A) IN GENERAL.—The term "covered information" means, with respect to an individual, any of the following:

(i) the first name or initial and last name;

(ii) a postal address;

(iii) an email address;

(iv) a telephone or fax number;

(v) a tax identification number, passport number, driver's license number, or any other unique government-issued identification number;

(vi) a financial account number, or credit card or debit card number, or any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(vii) any unique persistent identifier, such as a customer number, unique pseudonym or user alias, IP address, or other unique identifier, where such identifier is used to collect, store or identify information about a specific individual or to create or maintain a preference profile; or

(viii) any other information that is collected, stored, used, or disclosed in connection with any covered information described in clauses (i) through (vii).

(B) EXCLUSION.—Such term shall not include—

(i) the title, business address, business email address, business telephone number, or business fax number associated with an individual's status as an employee of an organization, or an individual's name when collected, stored, used, or disclosed in connection with such employment status; or

(ii) any information collected from or about an employee by an employer, prospective employer, or former employer that directly relates to the employee-employer relationship.

(5) OPERATIONAL PURPOSE.—

(A) IN GENERAL.—The term "operational purpose" means a purpose reasonably necessary to facilitate, improve, or safeguard the logistical or technical ability of a covered entity to provide goods or services, manage its operations, comply with legal obligations, or protect against risks and threats, including—

(i) providing, operating, or improving a product or service used, requested, or authorized by an individual, including the ongoing provision of customer service and support;

(ii) analyzing data related to use of the product or service for purposes of improving the covered entity's products, services, or operations;

(iii) basic business functions such as accounting, inventory and supply chain management, quality assurance, and internal auditing;

(iv) protecting or defending the rights or property, including intellectual property, of the covered entity against actual or potential security threats, fraud, theft, unau-

thorized transactions, or other illegal activities;

(v) preventing imminent danger to the personal safety of an individual or group of individuals;

(vi) complying with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(vii) any other category of operational use specified by the Commission by regulation that is consistent with the purposes of this Act.

(B) EXCLUSION.—Such term shall not include—

(i) the use of covered information for marketing or advertising purposes, or any use of or disclosure of covered information to a third party for such purposes; or

(ii) the use of covered information for a purpose that an individual acting reasonably under the circumstances would not expect based on the product or service used,

requested, or authorized by the individual and, if known to the individual, would likely affect the individual's conduct or decisions with respect to the covered entity's products or services.

(6) PREFERENCE PROFILE.—The term "preference profile" means a list of preferences, categories of information, or interests—

(A) associated with an individual or with an individual's computer or other device;

(B) inferred from the actual behavior of the individual, the actual use of the individual's computer or other device, or information supplied directly by the individual or other user of a computer or other device; and

(C) compiled and maintained for the purpose of marketing or purposes related to marketing, advertising, or sales.

(7) PUBLICLY AVAILABLE INFORMATION.—

(A) IN GENERAL.—The term "publicly available information" means any covered information or sensitive information that a covered entity has a reasonable basis to believe is lawfully made available to the general public from—

(i) Federal, State, or local government records;

(ii) widely distributed media; or

(iii) disclosures to the general public that are required to be made by Federal, State, or local law.

(B) CONSTRUCTION.—A covered entity has a reasonable basis to believe that information is lawfully made available to the general public if the covered entity has taken steps to determine—

(i) that the information is of a type that is available to the general public; and

(ii) whether an individual can direct that the information not be made available to the general public and, if so, that the individual has not done so.

(8) SENSITIVE INFORMATION.—

(A) DEFINITION.—The term "sensitive information" means—

(i) any information that is associated with covered information of an individual and relates directly to that individual's—

(I) medical history, physical or mental health, or the provision of health care to the individual;

(II) race or ethnicity;

(III) religious beliefs and affiliation;

(IV) sexual orientation or sexual behavior;

(V) income, assets, liabilities, or financial records, and other financial information associated with a financial account, including balances and other financial information, except when financial account information is provided by the individual and is used only to process an authorized credit or debit to the account; or

(VI) precise geolocation information and any information about the individual's activities and relationships associated with such geolocation; or

(ii) an individual's—

(I) unique biometric data, including a fingerprint or retina scan; or

(II) Social Security number.

(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by regulations promulgated under section 553 of title 5, United States Code, modify the scope or application of the definition of "sensitive information" for purposes of this Act. In promulgating such regulations, the Commission shall consider—

(i) the purposes of the collection of the information and the context of the use of the information;

(ii) how easily the information can be used to identify a specific individual;

(iii) the nature and extent of authorized access to the information;

(iv) an individual's reasonable expectations under the circumstances; and

(v) adverse effects that may be experienced by an individual if the information is disclosed to an unauthorized person.

(9) SERVICE PROVIDER.—The term "service provider" means an entity that collects, maintains, processes, stores, or otherwise handles covered information or sensitive information on behalf of a covered entity, including, for the purposes of serving as

a data processing center, distributing the information, providing customer support, maintaining the covered entity's records, information technology management, website or other hosting service, fraud detection, authentication, and other verification services, or performing other administrative support functions for the covered entity.

(10) THIRD PARTY.—

(A) IN GENERAL.—The term "third party" means, with respect to any covered entity, a person that—

(i) is not related to the covered entity by common ownership or corporate control; or

(ii) is a business unit or corporate entity that holds itself out to the public as separate from the covered entity, such that an individual acting reasonably under the circumstances would not expect it to be related to the covered entity or to have access to covered information the individual provides to that covered entity.

(B) COLLECTION OF INFORMATION BY MULTIPLE SOURCES.—For the purpose of this definition, where multiple persons collect cov-

ered information or sensitive information from or about visitors to an online or mobile service, including a website, all such persons other than the operator or publisher of the online or mobile service or website shall be considered third parties unless—

(i) the person meets the requirements of the service provider exception in section 106(1); or

(ii) the person otherwise does not satisfy the requirements for a third party pursuant to the regulations implemented pursuant to subparagraph (C).

(C) RULEMAKING.—Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to clarify or modify the definition of third party for purposes of this Act. In promulgating such regulations, the Commission shall consider—

(i) the brand or brands associated with a covered entity;

(ii) the scope and nature of the businesses engaged in by a covered entity and

a third party, including the nature of the products or services offered by the covered entity and third party; and

(iii) the relationship between a covered entity and a third party, taking into account such factors as ownership and control.

TITLE I—TRANSPARENCY, NOTICE, AND INDIVIDUAL CHOICE

SEC. 101. INFORMATION TO BE MADE AVAILABLE.

A covered entity shall, in accordance with the regulations issued under section 102, make available to individuals whose covered information or sensitive information it collects or maintains the following information about its information privacy practices and an individual's options with regard to such practices:

(1) The identity of the covered entity.

(2) A description of any covered information or sensitive information collected or stored by the covered entity.

(3) The specific purposes for which the covered entity collects and uses the covered information or sensitive information, including disclosure as to whether and how the covered entity customizes prod-

ucts or services or changes the prices of products or services based, in whole or in part, on covered information or sensitive information about individual customers or users.

(4) The specific purposes for which covered information or sensitive information may be disclosed to a third party and the categories of third parties who may receive such information for each such purpose.

(5) The choice and means the covered entity offers individuals for limiting the collection, use, and disclosure of covered information or sensitive information, in accordance with sections 103 and 104.

(6) A description of the information for which an individual may request access and the means to request such access, in accordance with section 202.

(7) How the covered entity may merge, link, or combine covered information or sensitive information collected from the individual with other information about the individual that the covered entity may acquire from third parties.

(8) The retention schedule for covered information and sensitive information in days, months, or years, or a statement that the covered entity will retain such information indefinitely or permanently.

(9) Whether or not an individual has the right to direct the covered entity to delete information collected from or about the individual.

(10) A reasonable means by which an individual may contact the covered entity with any inquiries or complaints regarding the covered entity's practices concerning the collection, use, disclosure, or handling of the individual's covered information or sensitive information in accordance with section 302(a).

(11) The process by which the covered entity notifies individuals of material changes to its policies and practices.

(12) A hyperlink to or a listing of the Commission's online consumer complaint form or the toll-free number for the Commission's Consumer Response Center.

(13) The effective date of the privacy notice.

SEC. 102. PROVISION OF NOTICE OR NOTICES.

(a) IN GENERAL.—It shall be unlawful for a covered entity to collect, use, or disclose covered information or sensitive information unless it provides the information set forth in section 101 in concise, meaningful, timely, prominent, and easy-to-understand notice or notices, in accordance with the regulations issued by the Commission under subsection (b).

(b) RULEMAKING.—Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In promulgating such regulations, the Commission—

(1) shall determine the means and timing of the notices required under this section, taking into account the different media, devices, or methods through which the covered entity collects covered information or sensitive information;

(2) shall have the authority to allow for, or require, the provision of short notices or limited disclosures that do not include all of the information set forth in section 101, if the Commission by regulation—

(A) requires the information to be otherwise clearly and conspicuously disclosed or available to individuals; and

(B) determines that the provision of such short notices or limited disclosures will accomplish the purposes of this Act to enhance transparency and provide individuals with meaningful choice regarding the collection, use, and disclosure of their covered information or sensitive information;

(3) shall consider—

(A) whether the notice or notices provide individuals with timely, effective, and meaningful notice that will enable an individual to understand relevant information and make informed choices;

(B) whether providing notice to individuals prior to or contemporaneously with the collection of covered information is practical or reasonable under the circumstances;

(C) the costs of implementing the prescribed notice or notices;

(D) the different media and context through which covered information is collected;

(E) whether it is reasonable and appropriate under the circumstances for a third party or a service provider to be responsible for providing notice and obtaining consent as required by this title in lieu of a covered entity; and

(F) the risk to consumers and commerce of over-notification; and

(4) may issue model notices.

(c) EXCLUSION FROM NOTICE REQUIREMENTS.—

(1) TRADE SECRET INFORMATION.—Nothing in this section shall require a covered entity to reveal confidential, trade secret, or proprietary information.

(2) IN-PERSON TRANSACTIONS.—Notice under this section shall not be required for in-person collection of covered information if—

(A) the covered information is collected for an operational purpose; or

(B) the covered entity only is collecting the name, address, email address, telephone or fax number of an individual and does not—

(i) share the covered information with third parties; or

(ii) use the covered information to acquire additional information about the individual from third parties.

(d) RETENTION.—A covered entity shall retain copies of the notice or notices issued pursuant to this section for a period of 6 years after the date on which such notice was issued or the date when it was last in effect, whichever is later, unless the Commission determines pursuant to the rulemaking required under subsection (b) that such retention is not practical under the circumstances.

SEC. 103. OPT-OUT CONSENT REQUIRED FOR COLLECTION AND USE OF COVERED INFORMATION BY A COVERED ENTITY.

(a) IN GENERAL.—Except as provided in subsections (e) and (f) and section 106, it shall be unlawful for a covered entity to collect or use covered information about an individual without the consent of that individual, as set forth in this section. A covered entity shall be considered to have the consent of an individual for the collection and use of covered information about the individual if—

(1) the covered entity has provided to the individual notice required under section 102 and its implementing regulations;

(2) the covered entity provides the individual with a reasonable means to exercise an opt-out right and decline consent for such collection and use; and

(3) the individual either affirmatively grants consent for such collection and use or does not decline consent at the time notice is presented or made available to the individual.

(b) DURATION OF INDIVIDUAL'S OPT-OUT.—An individual's direction to opt out under this section is effective permanently, unless otherwise directed by the individual.

(c) SUBSEQUENT OPT-OUT.—A covered entity shall provide an individual with a reasonable means to decline consent or revoke previously granted consent at any time.

(d) MORE DETAILED OPTIONS.—A covered entity may comply with this section by enabling an individual to decline consent for specific uses of his or her covered information, provided the individual has been given the opportunity to decline consent for the collection and use of covered information for all purposes, other than for an operational purpose excepted by subsection (e), for which covered information may be collected and used by the covered entity.

(e) EXCEPTION FOR OPERATIONAL PURPOSES.—This section shall not apply to the collection or use of covered information for an operational purpose.

(f) COLLECTION AND USE AS A CONDITION OF SERVICE.—Nothing in this section shall prohibit a covered entity from requiring, as a condition of an individual's receipt of a service or other benefit, including the receipt of an enhanced or premium version of a product or service otherwise available, the reasonable collection and use of covered information about the individual, provided that—

(1) the covered entity has a direct relationship with the individual;

(2) the covered information is not shared with any third party except with the express affirmative consent as set forth in section 104;

(3) the covered entity provides a clear, prominent, and specific statement describing the specific purpose or purposes for which covered information may be used pursuant to section 101;

(4) the individual provides consent by acknowledging the specific uses set forth in the clear and prominent statement required under paragraph (3) as part of receiving the service or other benefit from the covered entity; and

(5) the individual is able to later withdraw consent for the use by canceling the service or otherwise indicating that he or she no longer wishes to receive the service or other benefit.

SEC. 104. EXPRESS AFFIRMATIVE CONSENT.

(a) DISCLOSURE OF COVERED INFORMATION TO THIRD PARTIES.—

(1) DISCLOSURE PROHIBITED.—Except as provided in section 106 and subject to title IV of this Act, it shall be unlawful for a covered entity to disclose covered information about an individual to a third party unless the covered entity has received express affirmative consent from the individual prior to the disclosure.

(2) EXCEPTION FOR JOINT MARKETING.—Express affirmative consent shall not be required for

any disclosure related to the performance of joint marketing, if the covered entity and the third party enter into a contractual agreement prohibiting the third party from disclosing or using the covered information except as necessary to carry out the joint marketing relationship.

(b) COLLECTION, USE, OR DISCLOSURE OF SENSITIVE INFORMATION.—Except as provided in section 106, a covered entity may not collect, use, or disclose sensitive information from or about an individual for any purpose unless the covered entity obtains the express affirmative consent of the individual.

(c) COMPREHENSIVE ONLINE DATA COLLECTION.—A covered entity may not use hardware or software to monitor all or substantially all of the individual's Internet browsing or other significant class of Internet or computer activity and collect, use, or disclose information concerning such activity, except—

(1) with the express affirmative consent of the individual;

(2) for the purpose of making such information accessible to the individual or for use by the individual; or

(3) as provided in section 106.

(d) LIMITATION.—A third party that receives covered information or sensitive information from a covered entity pursuant to this section shall only use such information for the specific purposes authorized by the individual when the individual granted express affirmative consent for the disclosure of the information to a third party.

(e) REVOCATION OF CONSENT.—A covered entity that has obtained the express affirmative consent of an individual pursuant to this section and section 105 shall provide the individual with a reasonable means, without charge, to withdraw consent at any time thereafter.

SEC. 105. MATERIAL CHANGES TO PRIVACY PRACTICES.

(a) RETROACTIVE APPLICATION.—A covered entity shall provide the notice required by section 102 and obtain the express affirmative consent of the individual prior to making a material change in privacy practices governing previously collected covered information or sensitive information from that individual.

(b) PROSPECTIVE APPLICATION.—A covered entity shall not make material changes to its privacy practices governing the collection, use, or disclosure of covered information or sensitive information that has not been previously collected unless, 30 days before the effective date of the material change—

(1) the covered entity provides individuals with notice of the material change in accordance with section 102; and

(2) if required by sections 103 and 104, obtains the individual's consent to the material change or allows the individual to terminate the individual's relationship with the covered entity.

SEC. 106. EXCEPTIONS.

The consent requirements of sections 103 and 104 shall not apply to the following:

(1) SERVICE PROVIDERS.—

(A) When a covered entity discloses covered information or sensitive information to a service provider performing services or functions on behalf of and under the instruction of the covered entity, provided—

(i) the covered entity obtained the required consent for the initial collection of such information and provided notice as required by section 102;

(ii) the covered entity enters into a contractual agreement that prohibits the service provider from using or disclosing the information other than to carry out the

purposes for which the information was disclosed; and

(iii) in such cases, the covered entity remains responsible and liable for the protection of covered information and sensitive information that has been transferred to a service provider for processing.

(B) When a service provider subsequently discloses the information to another service provider in order to perform the same services or functions described in paragraph (1) on behalf of the covered entity.

(2) FRAUD DETECTION.—Collection, use, or disclosure necessary to protect or defend the rights or property, including intellectual property, of the covered entity against actual or potential security threats, fraud, theft, unauthorized transactions, or other illegal activities.

(3) IMMINENT DANGER.—Collection, use, or disclosure necessary to prevent imminent danger to the personal safety of an individual or group of individuals.

(4) COMPLIANCE WITH LAW.—Collection, use, or disclosure required in order to comply with a Federal, State, or local law, rule, or other applicable

legal requirement, including disclosures pursuant to subpoena, summons, or other properly executed compulsory process.

(5) PUBLICLY AVAILABLE INFORMATION.—Collection, use, or disclosure of publicly available information, except that a covered entity may not use publicly available information about an individual for marketing purposes if the individual has opted out of the use by such covered entity of covered information or sensitive information for marketing purposes.

TITLE II—ACCURACY, ACCESS, AND DISPUTE RESOLUTION

SEC. 201. ACCURACY.

(a) REASONABLE PROCEDURES.—Each covered entity shall establish reasonable procedures to assure the accuracy of the covered information or sensitive information it collects, assembles, or maintains. Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In promulgating such regulations, the Commission shall consider—

(1) the costs and benefits of ensuring the accuracy of the information;

(2) the sensitivity of the information;

(3) the purposes for which the information will be used; and

(4) the harms from misuse of the information.

(b) LIMITED EXCEPTION FOR FRAUD DATABASES.—The requirement in subsection (a) shall not prevent the collection or maintenance of information that may be inaccurate with respect to a particular individual when that information is being collected or maintained solely—

(1) for the purpose of indicating whether there may be a discrepancy or irregularity in the covered information or sensitive information that is associated with an individual; and

(2) to help identify, or authenticate the identity of, an individual, or to protect against or investigate fraud or other unlawful conduct.

(c) LIMITED EXCEPTION FOR PUBLICLY AVAILABLE INFORMATION.—Subject to section 202, a covered entity shall not be required to verify the accuracy of publicly available information if the covered entity has reasonable procedures to ensure that the publicly available information assembled or maintained by the covered entity accurately reflects the information available to the general public.

SEC. 202. ACCESS AND DISPUTE RESOLUTION.

(a) ACCESS AND CORRECTION.—A covered entity shall, upon request, provide an individual with reasonable access to, and the ability to dispute the accuracy or completeness of, covered information or sensitive information about that individual if such information may be used for purposes that could result in an adverse decision against the individual, including the denial of a right, benefit, or privilege.

(b) ACCESS TO PERSONAL PROFILES.—

(1) IN GENERAL.—Subject to title IV, a covered entity shall, upon request, provide an individual with reasonable access to any personal profile about that individual that the entity stores in a manner that makes it accessible in the normal course of business.

(2) SPECIAL RULE FOR PREFERENCE PROFILES.—With respect to a preference profile, the obligation to provide access and correction under this section is met if the covered entity provides the ability to review and change the preference information associated with a unique persistent identifier.

(3) PARTICIPATION IN CHOICE PROGRAM.—This subsection shall not apply to a covered entity that participates in a Choice Program under title IV.

(c) NOTICE IN LIEU OF ACCESS.—Subject to subsection (b), in those instances in which covered informa-

tion or sensitive information is used only for purposes that could not reasonably result in an adverse decision against an individual, including the denial of a right, benefit, or privilege, a covered entity shall, upon request by an individual, provide the individual with a general notice or representative sample of the type or types of information the covered entity typically collects or stores for such purposes.

(d) EXCEPTIONS.—

(1) A covered entity may decline to provide an individual with access to covered information or sensitive information if the covered entity reasonably believes—

(A) the individual requesting access cannot reasonably verify his or her identity as the person to which the information relates;

(B) access by the individual to the information is limited by law or legally recognized privilege;

(C) the information is used for a legitimate governmental or fraud prevention purpose that would be compromised by such access;

(D) such request for access is frivolous or vexatious;

(E) the privacy or other rights of persons other than the individual would be violated; or

(F) proprietary or confidential information, technology, or business processes would be revealed as a result.

(2) Where an exception described in paragraph (1) applies only to a portion of the covered information or sensitive information maintained by the covered entity, the covered entity shall provide access required under subsections (a) and (b) to the information to which the exception does not apply.

(3) A covered entity may decline an individual's request to correct or amend covered information or sensitive information pertaining to that individual where—

(A) a reason for denying access to the information under paragraph (1) would also apply to the request to correct or amend the information; or

(B) doing so would be incompatible with a legal obligation, such as a requirement to retain certain information.

(e) FEES.—A covered entity may charge a reasonable fee, as determined by the Commission, for providing access in accordance with subsection (a) or (b).

(f) TIME LIMIT.—A covered entity shall respond to any access, correction, or amendment request within 30 days of the receipt of the request. Such response must consist of one or more of the following:

(1) The requested information in accordance with subsection (a) or (b).

(2) The general notice in accordance with subsection (c).

(3) Instructions for accessing, correcting, or amending the requested information through an automated mechanism.

(4) A confirmation that the requested corrections or amendments have been made.

(5) A notification that the covered entity is declining to correct or amend information pursuant to one of the exceptions described in subsection (d). Such notification shall include the reason or reasons for not making the suggested correction or amendment, unless one or more of such exceptions would also apply to the disclosure of the reason or reasons.

(6) A request to resubmit the access request and an explanation of why the original access request was deficient in cases where—

(A) the scope or nature of the request is unclear or the entity needs more information in order to respond to the request;

(B) the entity charges a fee as permitted under subsection (e), and the fee has not been paid; or

(C) the entity provides interested members of the public other reasonable and accessible instructions for submitting an access request and such instructions were not followed.

(7) A notification that additional time is needed where—

(A) the entity cannot reasonably provide a full response within 30 days of the receipt of the access; and

(B) the time extension needed for a full response is no greater than an additional 30 days.

(g) RULE OF CONSTRUCTION.—Nothing in this Act creates an obligation on a covered entity to provide an individual with the right to delete information.

(h) ADDITIONAL REQUIREMENTS WHERE CORRECTION OR AMENDMENT IS DECLINED.—If the covered entity declines to correct or amend the information described in subsection (a), the covered entity shall—

(1) note that the information is disputed, including the individual's statement disputing such information, and take reasonable steps to verify such information under the procedures outlined in section 201 if such information can be independently verified; and

(2) where the information was obtained from a third party or is publicly available information, inform the individual of the source of the information, and if reasonably available, where a request for correction may be directed, and, if the individual provides proof that the information is incorrect, correct the inaccuracy in the covered entity's records.

(i) OTHER LIMITATIONS.—The obligations under this section do not, by themselves, create any obligation on the covered entity to retain, maintain, reorganize, or restructure covered information or sensitive information.

(j) DATA RETENTION EXCEPTION.—Covered information or sensitive information retained by the covered entity for under 30 days, or such other period of time as the Commission may determine, shall not be subject to this section.

(k) RULEMAKING.—Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5,

United States Code, to implement this section. In addition, the Commission shall promulgate regulations, as necessary, on the application of the exceptions and limitations in subsection (d), including any additional circumstances in which a covered entity may limit access to information under such subsection that the Commission determines to be appropriate.

TITLE III—DATA SECURITY, DATA MINIMIZATION, AND ACCOUNTABILITY

SEC. 301. DATA SECURITY.

(a) IN GENERAL.—Each covered entity and service provider shall establish, implement, and maintain reasonable and appropriate administrative, technical, and physical safeguards to—

(1) ensure the security, integrity, and confidentiality of the covered information or sensitive information it collects, assembles, or maintains;

(2) protect against any anticipated threats, reasonably foreseeable vulnerabilities, or hazards to the security or integrity of such information; and

(3) protect against unauthorized access to or use of such information and loss, misuse, alteration, or destruction of such information.

(b) FACTORS FOR APPROPRIATE SAFEGUARDS.—Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section. In promulgating such regulations, the Commission shall consider—

(1) the size and complexity of an entity;

(2) the nature and scope of the activities of an entity;

(3) the sensitivity of the information;

(4) the current state of the art in administrative, technical, and physical safeguards for protecting information; and

(5) the cost of implementing such safeguards.

SEC. 302. ACCOUNTABILITY.

(a) COMPLAINTS TO THE COVERED ENTITY.—A covered entity shall provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this Act.

(b) PRIVACY RISK ASSESSMENT.—A covered entity shall conduct an assessment of the risks to individuals raised by the collection, use, and disclosure of covered information or sensitive information prior to the implementation of commercial projects, marketing initiatives, business models, applications, and other products or services

in which the covered entity intends to collect, or believes there is a reasonable likelihood it will collect, covered information or sensitive information from or about more than 1,000,000 individuals.

(c) PERIODIC EVALUATION OF PRACTICES.—A covered entity shall conduct periodic assessments to evaluate—

(1) whether the covered information or sensitive information the covered entity has collected is and remains necessary for the purposes disclosed at the time of collection pursuant to section 101 (c) and (d); and

(2) whether the covered entity's ongoing collection practices are and remain necessary for a legitimate business purpose.

SEC. 303. DATA MINIMIZATION OBLIGATIONS.

A covered entity that uses covered information or sensitive information for any purpose shall retain such data only as long as necessary to fulfill a legitimate business purpose or comply with a legal requirement.

TITLE IV—SAFE HARBOR AND SELF-REGULATORY CHOICE PROGRAM

SEC. 401. SAFE HARBOR.

A covered entity that participates in, and is in compliance with, 1 or more self-regulatory programs approved by the Commission under section 402 (in this title referred to as a "Choice Program") shall not be subject to—

(1) the requirements for express affirmative consent required under subsection 104(a) for the specified uses of covered information addressed by the Choice Program as described in section 403(1)(A);

(2) the requirement of access to information under section 202(b); or

(3) liability in a private right of action brought under section 604.

SEC. 402. APPROVAL BY THE FEDERAL TRADE COMMISSION.

(a) INITIAL APPROVAL.—Not later than 270 days after the submission of an application for approval of a Choice Program under this section, the Commission shall approve or decline to approve such program. The Commission shall only approve such program if the Commission

finds, after notice and comment, that the program complies with the requirements of section 403.

(b) APPROVAL OF MODIFICATIONS.—The Commission shall approve or decline to approve any material change in a Choice Program previously approved by the Commission within 120 days after submission of an application for approval by such program. The Commission shall only approve such material change if the Commission finds, after notice and comment, that the proposed change complies with the requirements of section 403.

(c) DURATION.—A Choice Program approved by the Commission under this section shall be approved for a period of 5 years.

(d) APPEALS.—Final action by the Commission on a request for approval, or the failure to act within 270 days on a request for approval, submitted under this section may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5, United States Code.

SEC. 403. REQUIREMENTS OF SELF-REGULATORY PROGRAM.

To be approved as a Choice Program under this section, a program shall—

(1) provide individuals with—

(A) a clear and conspicuous opt-out mechanism that, when selected by the individual, prohibits all covered entities participating in the Choice Program from disclosing covered information to a third party for 1 or more specified uses, and may offer individuals a preference management tool that will enable an individual to make more detailed choices about the transfer of covered information to a third party; and

(B) a clear and conspicuous mechanism to set communication preferences, online behavioral advertising preferences, and such other preferences as the Choice Program may determine, subject to the approval of the Commission, that when selected by the individual, applies the individual's selected preferences to all covered entities participating in the Choice Program; and

(2) establish—

(A) guidelines and procedures requiring a participating covered entity to provide equivalent or greater protections for individuals and their covered information and sensitive information as are provided under titles I and II;

(B) procedures for reviewing applications by covered entities to participate in the Choice Program;

(C) procedures for periodic assessment of its procedures and for conducting periodic random compliance testing of covered entities participating in such Choice Program; and

(D) consequences for failure to comply with program requirements, such as public notice of the covered entity's noncompliance, suspension, or expulsion from the program, or referral to the Commission for enforcement.

SEC. 404. RULEMAKING.

Not later than 18 months after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement this section and to provide compliance guidance for entities seeking to be approved under this title, including regulations—

(1) establishing criteria for the submission of the application, including evidence of how the Choice Program will comply with the requirements of section 403;

(2) establishing criteria for opt-out mechanisms and communication preferences, online behavioral

advertising preferences, or other preferences meeting the requirements of this title;

(3) establishing consequences for failure to comply with the requirements of section 403, such as public notice of the Choice Program's noncompliance and suspension or revocation of the Commission's approval of such Program as described in section 402;

(4) allowing for and promoting continued evolution and innovation in privacy protection, meaningful consumer control, simplified approaches to disclosure, and transparency; and

(5) providing additional incentives for self-regulation by covered entities to implement the protections afforded individuals under titles I and II of this Act, including provisions for ensuring that a covered entity will be considered to be in compliance with the requirements of titles I and II and the regulations issued under such titles if that covered entity complies with guidelines or requirements of a Choice Program approved under section 402.

TITLE V—EXEMPTIONS

SEC. 501. USE OF AGGREGATE OR DEIDENTIFIED INFORMATION.

(a) GENERAL EXCLUSION.—Subject to subsections (b) and (c), nothing in this Act shall preclude a covered entity from collecting, using, or disclosing—

(1) aggregate information; or

(2) covered information or sensitive information from which identifying information has been obscured or removed using reasonable and appropriate methods such that the remaining information does not identify, and there is no reasonable basis to believe that the information can be used to identify—

(A) the specific individual to whom such covered information relates; or

(B) a computer or device owned or used by a specific individual.

(b) REASONABLE PROCEDURES FOR DISCLOSURE.—If a covered entity discloses the information described in paragraphs (1) and (2) of subsection (a) to a third party, the covered entity shall take reasonable steps to protect such information, including, in the case of the information described in such paragraph (2), not disclosing the algorithm or other mechanism used to obscure or remove the identifying information, and obtaining satisfactory written

assurance that the third party will not attempt to reconstruct the identifying information.

(c) PROHIBITION ON RECONSTRUCTING OR REVEALING IDENTIFYING INFORMATION.—

(1) IN GENERAL.—It shall be unlawful for any person to reconstruct or reveal the identifying information that has been removed or obscured (as described in subsection (a)(2)) and for which a covered entity claims or has claimed the benefit of the general exemption in subsection (a).

(2) RULEMAKING.—Not later than 18 months after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish exemptions to this subsection. In promulgating such regulations, the Commission shall consider—

(A) the purposes for which such identifying information may need to be reconstructed or revealed;

(B) the size and sensitivity of the data set; and

(C) public policy issues such as health, safety, and national security.

SEC. 502. ACTIVITIES COVERED BY OTHER FEDERAL PRIVACY LAWS.

Except as provided expressly in this Act, this Act shall have no effect on activities covered by any of the following:

(1) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(2) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(3) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191).

(4) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).

(5) Sections 222 and 631 of the Communications Act of 1934 (47 U.S.C. 222 and 47 U.S.C. 551).

(6) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(7) The CAN–SPAM Act of 2003 (15 U.S.C. 7701 et seq.).

(8) The Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 et seq.).

(9) The Video Privacy Protection Act (18 U.S.C. 2710 et seq.).

TITLE VI—APPLICATION AND ENFORCEMENT

SEC. 601. GENERAL APPLICATION.

The requirements of this Act shall only apply to those persons over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act. Notwithstanding any provision of such Act or any other provision of law, common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and any amendment thereto shall be subject to the jurisdiction of the Commission for purposes of this Act.

SEC. 602. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of titles I, II, or III shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(b) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person

who violates this Act or the regulations issued under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(c) RULEMAKING AUTHORITY.—

(1) RULEMAKING.—The Commission may, in accordance with section 553 of title 5, United States Code, issue such regulations it determines to be necessary to carry out this Act.

(2) AUTHORITY TO GRANT EXCEPTIONS.—The regulations prescribed under paragraph (1) may include such additional exceptions to titles I, II, III, IV, and V of this Act as the Commission considers consistent with the purposes of this Act.

(3) LIMITATION.—In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

SEC. 603. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) CIVIL ACTION.—In any case in which the Attorney General of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates this Act, the attorney general, official, or agency of the State, as parens patriae, may

bring a civil action on behalf of the residents of the State in an appropriate district court of the United States—

(1) to enjoin further violation of this Act by the defendant;

(2) to compel compliance with this Act; or

(3) for violations of titles I, II, or III of this Act, to obtain civil penalties in the amount determined under subsection (b).

(b) CIVIL PENALTIES.—

(1) CALCULATION.—For purposes of calculating the civil penalties that may be obtained under subsection (a)(3)—

(A) with regard to a violation of title I, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such title, or the number of individuals for whom the covered entity failed to obtain consent as required by such title, whichever is greater, by an amount not to exceed $11,000; and

(B) with regard to a violation of title II or III, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not

in compliance with such title or titles by an amount not to exceed $11,000.

(2) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index for All Urban Consumers is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in subparagraphs (A) and (B) of paragraph (1) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(3) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a person under this section the maximum civil penalty for which any person may be liable under this section shall not exceed—

(A) $5,000,000 for any related series of violations of title I; and

(B) $5,000,000 for any related series of violations of title II and title III.

(4) EFFECT OF PARTICIPATION IN CHOICE PROGRAM.—If a covered entity participates in a Choice Program established under title IV and cures the alleged violation of title I or II in a reasonable period

of time after receiving notice of the alleged violation, such conduct shall be taken into consideration by a State or a court in determining the amount of civil penalties under this subsection.

(c) INTERVENTION BY THE FTC.—

(1) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under subsection (a) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein; and

(C) to file petitions for appeal.

(2) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no attorney general of a State, or official, or agency of a State, may bring an action under this section during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 604. PRIVATE RIGHT OF ACTION.

(a) IN GENERAL.—A covered entity, other than a covered entity that participates in and is in compliance with a Choice Program established under title IV, who willfully fails to comply with sections 103 or 104 of this Act with respect to any individual is liable to that individual in a civil action brought in a district court of the United States of appropriate jurisdiction in an amount equal to the sum of—

(1) the greater of any actual damages of not less than $100 and not more than $1,000;

(2) such amount of punitive damages as the court may allow; and

(3) in the case of any successful action under this section, the costs of the action together with

reasonable attorney's fees as determined by the court.

(b) LIMITATION.—A civil action under this section may not be commenced later than 2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

SEC. 605. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly requires covered entities to implement requirements with respect to the collection, use, or disclosure of covered information addressed in this Act.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 603 or 604 may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF STATE CONSUMER PROTECTION LAWS.—This subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general or other official of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

(1) State laws that address the collection, use, or disclosure of health information or financial information;

(2) State laws that address notification requirements in the event of a data breach;

(3) State trespass, contract, or tort law; or

(4) other State laws to the extent that those laws relate to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any provision of law.

(e) RULE OF CONSTRUCTION RELATING TO REQUIRED DISCLOSURES TO GOVERNMENT ENTITIES.—This Act shall not be construed to expand or limit the duty or authority of a covered entity, service provider, or third party to disclose covered information or sensitive information to a government entity under any provision of law.

TITLE VII—MISCELLANEOUS PROVISIONS

SEC. 701. REVIEW.

Not later than 5 years after the effective date of the regulations initially issued under this Act, the Commission shall—

(1) review the implementation of this Act, including the effect of the implementation of this Act on practices relating to the collection, use, and disclosure of covered information and sensitive information; and

(2) prepare and submit to Congress a report on the results of the review under paragraph (1).

SEC. 702. CONSUMER AND BUSINESS EDUCATION CAMPAIGN.

Beginning on the effective date of this Act as set forth in section 703, the Commission shall—

(1) conduct a consumer education campaign to inform individuals of the rights and protections afforded by this Act and the steps that individuals can take to affirmatively consent or decline consent to the collection, use, and disclosure of information under this Act and the regulations issued pursuant to this Act; and

(2) provide guidance to businesses regarding their obligations under this Act, including guidance on how to participate in a Choice Program approved under title IV.

SEC. 703. EFFECTIVE DATE.

This Act shall take effect 2 years after the date of the enactment of this Act. The Commission may stay enforcement of this Act for such period of time as the Commission determines necessary to allow for the establishment and Commission approval of a Choice Program under title IV and for covered entities to commence participation in such a program.

SEC. 704. SEVERABILITY.

If any provision of this Act, or the application thereof to any person or circumstance, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other persons and circumstances shall not be affected thereby.

○

[STAFF DISCUSSION DRAFT]

MAY 3, 2010

111TH CONGRESS
1ST SESSION

H. R. _____

To require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

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 "[To be provided]".

SEC. 2. DEFINITIONS.

In this Act the following definitions apply:

(1) ADVERTISEMENT NETWORK.—The term '"advertisement network" means an entity that provides advertisements to participating websites on the basis of individuals' activity across some or all of those websites.

(2) AGGREGATE INFORMATION.—The term "aggregate information" means data that relates to a group or category of services or individuals, from which all information identifying an individual has been removed.

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) COVERED ENTITY.—The term "covered entity"—

(A) means a person engaged in interstate commerce that collects data containing covered information; and

(B) does not include—

(i) a government agency; or

(ii) any person that collects covered information from fewer than 5,000 individuals in any 12-month period and does not collect sensitive information.

(5) COVERED INFORMATION.—The term "covered information" means, with respect to an individual, any of the following:

(A) The first name or initial and last name.

(B) A postal address.

(C) A telephone or fax number.

(D) An email address.

(E) Unique biometric data, including a fingerprint or retina scan.

(F) A Social Security number, tax identification number, passport number, driver's license number, or any other government-issued identification number.

(G) A Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(H) Any unique persistent identifier, such as a customer number, unique pseudonym or user alias, Internet Protocol address, or other unique identifier, where such identifier is used to collect, store, or identify information about a specific individual or a computer, device, or

software application owned or used by a particular user or that is otherwise associated with a particular user.

(I) A preference profile.

(J) Any other information that is collected, stored, used, or disclosed in connection with any covered information described in subparagraphs (A) through (I).

(6) FIRST PARTY TRANSACTION.—The term "first party transaction" means an interaction between an entity that collects covered information when an individual visits that entity's website or place of business and the individual from whom covered information is collected.

(7) OPERATIONAL PURPOSE.—

(A) IN GENERAL.—The term "operational purpose" means a purpose reasonably necessary for the operation of the covered entity, including—

(i) providing, operating, or improving a product or service used, requested, or authorized by an individual;

(ii) detecting, preventing, or acting against actual or reasonably suspected threats to the covered entity's product or

service, including security attacks, unauthorized transactions, and fraud;

(iii) analyzing data related to use of the product or service for purposes of optimizing or improving the covered entity's products, services, or operations;

(iv) carrying out an employment relationship with an individual;

(v) disclosing covered information based on a good faith belief that such disclosure is necessary to comply with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(vi) disclosing covered information to a parent company of, controlled subsidiary of, or affiliate of the covered entity, or other covered entity under common control with the covered entity where the parent, subsidiary, affiliate, or other covered entity operates under a common or substantially similar set of internal policies and procedures as the covered entity, and the poli-

cies and procedures include adherence to the covered entity's privacy policies as set forth in its privacy notice.

(B) EXCLUSION.—Such term shall not include the use of covered information for marketing, advertising, or sales purposes, or any use of or disclosure of covered information to an unaffiliated party for such purposes.

(8) PREFERENCE PROFILE.—The term "preference profile" means a list of information, categories of information, or preferences associated with a specific individual or a computer or device owned or used by a particular user that is maintained by or relied upon by a covered entity.

(9) RENDER ANONYMOUS.—The term "render anonymous" means to remove or obscure covered information such that the remaining information does not identify, and there is no reasonable basis to believe that the information can be used to identify—

(A) the specific individual to whom such covered information relates; or

(B) a computer or device owned or used by a particular user.

(10) SENSITIVE INFORMATION.—The term "sensitive information" means any information that

is associated with covered information of an individual and relates to that individual's—

(A) medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(B) race or ethnicity;

(C) religious beliefs;

(D) sexual orientation;

(E) financial records and other financial information associated with a financial account, including balances and other financial information; or

(F) precise geolocation information.

(11) SERVICE PROVIDER.—The term "service provider" means an entity that collects, maintains, processes, stores, or otherwise handles covered information on behalf of a covered entity, including, for the purposes of serving as a data processing center, providing customer support, serving advertisements to the website of the covered entity, maintaining the covered entity's records, or performing other administrative support functions for the covered entity.

(12) TRANSACTIONAL PURPOSE.—The term "transactional purpose" means a purpose necessary

for effecting, administering, or enforcing a transaction between a covered entity and an individual.

(13) UNAFFILIATED PARTY.—The term "unaffiliated party" means any entity that is not related by common ownership or affiliated by corporate control with a covered entity.

SEC. 3. NOTICE AND CONSENT REQUIREMENTS FOR THE COLLECTION, USE, AND DISCLOSURE OF COVERED INFORMATION.

(a) NOTICE AND CONSENT PRIOR TO COLLECTION AND USE OF COVERED INFORMATION.—

(1) IN GENERAL.—A covered entity shall not collect, use, or disclose covered information from or about an individual for any purpose unless such covered entity—

(A) makes available to such individual the privacy notice described in paragraph (2) prior to the collection of any covered information; and

(B) obtains the consent of the individual to such collection as set forth in paragraph (3).

(2) NOTICE REQUIREMENTS.—

(A) NATURE OF NOTICE.—

(i) COLLECTION OF INFORMATION THROUGH THE INTERNET.—If the covered

entity collects covered information through the Internet, the privacy notice required by this section shall be—

(I) posted clearly and conspicuously on the website of such covered entity through which the covered information is collected; and

(II) accessible through a direct link from the Internet homepage of the covered entity.

(ii) MANUAL COLLECTION OF INFORMATION BY MEANS OTHER THAN THROUGH THE INTERNET.—If the covered entity collects covered information by any means that does not utilize the Internet, the privacy notice required by this section shall be made available to an individual in writing before the covered entity collects any covered information from that individual.

(B) REQUIRED INFORMATION.—The privacy notice required under paragraph (1) shall include the following information:

(i) The identity of the covered entity collecting the covered information.

(ii) A description of any covered information collected by the covered entity.

(iii) How the covered entity collects covered information.

(iv) The specific purposes for which the covered entity collects and uses covered information.

(v) How the covered entity stores covered information.

(vi) How the covered entity may merge, link, or combine covered information collected about the individual with other information about the individual that the covered entity may acquire from unaffiliated parties.

(vii) How long the covered entity retains covered information in identifiable form.

(viii) How the covered entity disposes of or renders anonymous covered information after the expiration of the retention period.

(ix) The purposes for which covered information may be disclosed, and the categories of unaffiliated parties who may re-

ceive such information for each such purpose.

(x) The choice and means the covered entity offers individuals to limit or prohibit the collection and disclosure of covered information, in accordance with this section.

(xi) The means by and the extent to which individuals may obtain access to covered information that has been collected by the covered entity in accordance with this section.

(xii) A means by which an individual may contact the covered entity with any inquiries or complaints regarding the covered entity's handling of covered information.

(xiii) The process by which the covered entity notifies individuals of material changes to its privacy notice in accordance with paragraph (4).

(xiv) A hyperlink to or a listing of the Commission's online consumer complaint form or the toll-free telephone number for the Commission's Consumer Response Center.

(xv) The effective date of the privacy notice.

(3) OPT-OUT CONSENT REQUIREMENTS.—

(A) OPT-OUT NATURE OF CONSENT.—A covered entity shall be considered to have the consent of an individual for the collection and use of covered information relating to that individual if—

(i) the covered entity has provided to the individual a clear statement containing the information required under paragraph (2)(B) and informing the individual that he or she has the right to decline consent to such collection and use; and

(ii) the individual either affirmatively grants consent for such collection and use or does not decline consent at the time such statement is presented to the individual.

If an individual declines consent at any time subsequent to the initial collection of covered information, the covered entity may not collect covered information from the individual or use covered information previously collected.

(B) ADDITIONAL OPTIONS AVAILABLE.—A covered entity may comply with this subsection by enabling an individual to decline consent for the collection and use only of particular covered information, provided the individual has been given the opportunity to decline consent for the collection and use of all covered information.

(4) NOTICE AND CONSENT TO MATERIAL CHANGE IN PRIVACY POLICIES.—A covered entity shall provide the privacy notice required by paragraph (2) and obtain the express affirmative consent of the individual prior to—

(A) making a material change in privacy practices governing previously collected covered information from that individual; or

(B) disclosing covered information for a purpose not previously disclosed to the individual and which the individual, acting reasonably under the circumstances, would not expect based on the covered entity's prior privacy notice.

(5) EXEMPTION FOR A TRANSACTIONAL PURPOSE OR AN OPERATIONAL PURPOSE.—

(A) EXEMPTION FROM NOTICE REQUIREMENTS.—The notice requirements in this sub-

section shall not apply to covered information that—

(i) is collected by any means that does not utilize the Internet, as described in paragraph (2)(A)(ii); and

(ii)(I) is collected for a transactional purpose or an operational purpose; or

(II) consists solely of information described in subparagraphs (A) through (D) of section 2(5) and is part of a first party transaction.

(B) EXEMPTION FROM CONSENT REQUIREMENTS.—The consent requirements of this subsection shall not apply to the collection, use, or disclosure of covered information for a transactional purpose or an operational purpose, but shall apply to the collection by a covered entity of covered information for marketing, advertising, or selling, or any use of or disclosure of covered information to an unaffiliated party for such purposes.

(b) EXPRESS CONSENT REQUIRED FOR DISCLOSURE OF COVERED INFORMATION TO UNAFFILIATED PARTIES.—

(1) IN GENERAL.—A covered entity may not sell, share, or otherwise disclose covered information to an unaffiliated party without first obtaining the express affirmative consent of the individual to whom the covered information relates.

(2) WITHDRAWAL OF CONSENT.—A covered entity that has obtained express affirmative consent from an individual must provide the individual with the opportunity, without charge, to withdraw such consent at any time thereafter.

(3) EXEMPTION FOR CERTAIN INFORMATION SHARING WITH SERVICE PROVIDERS.—The consent requirements of this subsection shall not apply to the disclosure of covered information by a covered entity to a service provider for purposes of executing a first party transaction if—

(A) the covered entity has obtained consent for the collection of covered information pursuant to subsection (a); and

(B) the service provider agrees to use such covered information solely for the purpose of providing an agreed-upon service to a covered entity and not to disclose the covered information to any other person.

(c) EXPRESS CONSENT FOR COLLECTION OR DISCLOSURE OF SENSITIVE INFORMATION.—A covered entity shall not collect or disclose sensitive information from or about an individual for any purpose unless such covered entity—

(1) makes available to such individual the privacy notice described in subsection (a)(2) prior to the collection of any sensitive information; and

(2) obtains the express affirmative consent of the individual to whom the sensitive information relates prior to collecting or disclosing such sensitive information.

(d) EXPRESS CONSENT FOR COLLECTION OR DISCLOSURE OF ALL OR SUBSTANTIALLY ALL OF AN INDIVIDUAL'S ONLINE ACTIVITY.—A covered entity shall not collect or disclose covered information about all or substantially all of an individual's online activity, including across websites, for any purpose unless such covered entity—

(1) makes available to such individual the privacy notice described in subsection (a)(2) prior to the collection of the covered information about all or substantially all of the individual's online activity; and

(2) obtains the express affirmative consent of the individual to whom the covered information relates prior to collecting or disclosing such covered information.

(e) EXCEPTION FOR INDIVIDUAL MANAGED PREFERENCE PROFILES.—Notwithstanding subsection (b), a covered entity may collect, use, and disclose covered information if—

(1) the covered entity provides individuals with the ability to opt out of the collection, use, and disclosure of covered information by the covered entity using a readily accessible opt-out mechanism whereby, the opt-out choice of the individual is preserved and protected from incidental or accidental deletion, including by—

(A) website interactions on the covered entity's website or a website where the preference profile is being used;

(B) a toll-free phone number; or

(C) letter to an address provided by the covered entity;

(2) the covered entity deletes or renders anonymous any covered information not later than 18 months after the date the covered information is first collected;

(3) the covered entity includes the placement of a symbol or seal in a prominent location on the website of the covered entity and on or near any advertisements delivered by the covered entity based on the preference profile of an individual that enables an individual to connect to additional information that—

(A) describes the practices used by the covered entity or by an advertisement network in which the covered entity participates to create a preference profile and that led to the delivery of the advertisement using an individual's preference profile, including the information, categories of information, or list of preferences associated with the individual that may have led to the delivery of the advertisement to that individual; and

(B) allows individuals to review and modify, or completely opt out of having, a preference profile created and maintained by a covered entity or by an advertisement network in which the covered entity participates; and

(4) an advertisement network to which a covered entity discloses covered information under this subsection does not disclose such covered informa-

tion to any other entity without the express affirmative consent of the individual to whom the covered information relates.

SEC. 4. ACCURACY AND SECURITY OF COVERED INFORMATION AND CONSUMER EDUCATION CAMPAIGN.

(a) ACCURACY.—Each covered entity shall establish reasonable procedures to assure the accuracy of the covered information it collects.

(b) SECURITY OF COVERED INFORMATION.—

(1) IN GENERAL.—A covered entity or service provider that collects covered information about an individual for any purpose must establish, implement, and maintain appropriate administrative, technical, and physical safeguards that the Commission determines are necessary to—

(A) ensure the security, integrity, and confidentiality of such information;

(B) protect against anticipated threats or hazards to the security or integrity of such information;

(C) protect against unauthorized access to and loss, misuse, alteration, or destruction of, such information; and

(D) in the event of a security breach, determine the scope of the breach, make every reasonable attempt to prevent further unauthorized access to the affected covered information, and restore reasonable integrity to the affected covered information.

(2) FACTORS FOR APPROPRIATE SAFEGUARDS.—In developing standards to carry out this section, the Commission shall consider the size and complexity of a covered entity, the nature and scope of the activities of a covered entity, the sensitivity of the covered information, the current state of the art in administrative, technical, and physical safeguards for protecting information, and the cost of implementing such safeguards.

(c) CONSUMER EDUCATION.—The Commission shall conduct a consumer education campaign to educate the public regarding opt-out and opt-in consent rights afforded by this Act.

SEC. 5. USE OF AGGREGATE OR ANONYMOUS INFORMATION.

Nothing in this Act shall prohibit a covered entity from collecting or disclosing aggregate information or covered information that has been rendered anonymous.

SEC. 6. USE OF LOCATION-BASED INFORMATION.

(a) IN GENERAL.—Except as provided in section 222(d) of the Communications Act of 1934 (47 U.S.C. 222(d)), any provider of a product or service that uses location-based information shall not disclose such location-based information concerning the user of such product or service without that user's express opt-in consent. A user's express opt-in consent to an application provider that relies on a platform offered by a commercial mobile service provider shall satisfy the requirements of this subsection.

(b) AMENDMENT.—Section 222(h) of the Communications Act of 1934 (47 U.S.C. 222(h)) is amended by adding at the end the following:

"(8) CALL LOCATION INFORMATION.—The term 'call location information' means any location-based information."

SEC. 7. FEDERAL COMMUNICATIONS COMMISSION REPORT.

Not later than 1 year after the date of enactment of this Act, the Federal Communications Commission shall transmit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate describing—

(1) all provisions of United States communications law, including provisions in the Communica-

tions Act of 1934, that address subscriber privacy; and

(2) how those provisions may be harmonized with the provisions of this Act to create a consistent regulatory regime for covered entities and individuals.

SEC. 8. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in

that Act. Notwithstanding any provision of the Federal Trade Commission Act or any other provision of law and solely for purposes of this Act, common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and any amendment thereto shall be subject to the jurisdiction of the Commission.

(3) RULEMAKING AUTHORITY AND LIMITATION.—The Commission may, in accordance with section 553 of title 5, United States Code, issue such regulations it determines to be necessary to carry out this Act. In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or agency of a State having consumer protection responsibilities, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates this Act, the attorney general or such agency of the State, as parens

patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin further violation of such section by the defendant;

(B) compel compliance with such section;

(C) obtain damage, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider appropriate.

(2) INTERVENTION BY THE FTC.—

(A) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no State attorney general or agency of a State may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(3) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 9. NO PRIVATE RIGHT OF ACTION.

This Act may not be considered or construed to provide any private right of action. No private civil action relating to any act or practice governed under this Act may be commenced or maintained in any State court or

under State law (including a pendent State claim to an action under Federal law).

SEC. 10. PREEMPTION.

This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, that includes requirements for the collection, use, or disclosure of covered information.

SEC. 11. EFFECT ON OTHER LAWS.

(a) APPLICATION OF OTHER FEDERAL PRIVACY LAWS.—Except as provided expressly in this Act, this Act shall have no effect on activities covered by the following:

(1) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(2) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(3) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).

(4) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).

(5) The Communications Act of 1934 (47 U.S.C. 151 et seq.).

(6) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(7) The CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.).

(b) COMMISSION AUTHORITY.—Nothing contained in this Act shall be construed to limit authority provided to the Commission under any other law.

SEC. 12. EFFECTIVE DATE.

Unless otherwise specified, this Act shall apply to the collection, use, or disclosure of, and other actions with respect to, covered information that occurs on or after the date that is one year after the date of enactment of this Act.

And now I recognize the Ranking Member of the Subcommittee, Mr. Whitfield, for 5 minutes for the purposes of an opening statement.

OPENING STATEMENT OF HON. ED WHITFIELD, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. WHITFIELD. Well, Chairman Rush, thank you very much and we certainly appreciate our panel of expert witnesses here today. As you know we are having this hearing to explore privacy legislation. I want to commend Chairman Rush for introducing his bill and want to thank him and his staff for giving us an opportunity to review that legislation. And all of us recognize that some steps need to be taken in this area, and we are hopeful that after today's hearing a lot of these issues will be clarified even more for us because as I said in the beginning we look forward to your testimony on this important issue.

It seems to me the threshold question is whether Congress can require meaningful protections without forcing businesses online and offline to abandon or severely curtail legitimate business practices that benefit consumers. We know that it is easy to misuse information, and we also know there are benefits from sharing information, so that balancing act is very important. The problem I believe for most consumers is the lack of understanding about how their information is collected, and once used how—and once they provide it how that is being used, and the impact that it has on them.

This is a preparatory hearing and we always have a lot of concerns about legislation, particularly when it is in the area of privacy. One of the areas that I have some concern about is that the first party, third party distinction created by this bill could also give certain players in the Internet ecosystem a competitive advantage over others, and I think we need a level playing field. I think it would be very difficult also for Congress to be involved of every nuance of privacy, and I think we need to be very careful about the latitude that we give the FTC in this area.

One of the areas that is vitally important obviously in policing any legislation is the enforcement mechanism. I am always concerned about private rights of action because I know in some instances it has really created a cottage industry for trial lawyers seeking to manufacture privacy concerns. But I also know that sometimes those appear to be—these private rights of actions seem to be a good way to go.

I do support the ability of State Attorneys General to enforce the Federal Statute. I don't think this bill goes far enough in terms of preempting state laws, creating the possibility that despite the bill's intent, covered entities would be subject to actions under multiple potentially conflicting laws or legal theories for conduct sanctioned by this bill.

Whatever Congress ultimately enacts consumers will not care really about the corporate structure or the regulatory regime that governs the entity collecting their information. They only want to be sure that their information is treated the same by all entities and that they have reasonable protection. And I feel quite confident

that when we enact privacy legislation that we will have a balanced bill that everyone will be satisfied with. Maybe I shouldn't say everyone, but most people will be satisfied with, and of course, that is our objective.

Now I yield back the balance of my time.

[The prepared statement of Mr. Whitfield follows:]

Statement of the Honorable Ed Whitfield

Ranking Member, Subcommittee on Commerce, Trade, and Consumer Protection

Hearing on Privacy Drafts

July 22, 2010

- Thank you for calling this hearing on two well intentioned pieces of legislation intended to address privacy protections for consumers. This is not an easy topic to legislate, but protections are overdue.

- I am glad we are able to assemble a panel of witnesses on short notice to comment on the two drafts and hope they can further enlighten us on the impact of these provisions.

- I think these are both good starting points for discussion as we try and tackle the best way to provide consumer with the information they need about what and how their information will be collected and used by commercial entities.

- The threshold question is whether we can provide meaningful protections without forcing businesses – online and offline – to start their business over from scratch. The proverbial "genie" is out of the bottle, allowing information to be collected, stored, and shared for various purposes on a daily basis, often unbeknownst to the consumer.

- That is not to say the information is always used for nefarious purposes. Indeed, there are many benefits that have accrued to consumers through customization and free services supported most often by advertisements.

- The problem for most consumers is the loss of control of their information once they surrender it in exchange for something of value, and who gets to use that information.

- My concerns after reviewing the drafts center on the consent provisions, the effect on different business models and the enforcement provisions.

- I believe the Federal Trade Commission and its track record as a consumer protection enforcement agency is best suited to be the Federal agency in charge. But I do have concerns about the private rights of action as an additional enforcement mechanism or deterrent.

- Whatever Congress ultimately enacts, consumers will not care about the corporate structure or the regulatory regime that governs the entity collecting their information. They only want to be sure their information is treated the same with every business with

whom they transact. If we keep that principle as a guiding tenet I am sure we can provide meaningful protections many consumers desire.

- Thank you

Mr. RUSH. We will be seeking everyone on this bill. We will now have Ms. Castor for 2 minutes.

OPENING STATEMENT OF HON. KATHY CASTOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Ms. CASTOR. Thank you, Chairman Rush, very much, and thank you to the witnesses for being here today. I am looking forward to your discussion of consumer privacy in the Internet age, and such an exciting age of technological innovation. And I hope your comments will be directed to the two draft discussion bills that are on the table. We need your expert advice on how we balance the important competing interests of personal privacy and business innovation.

We do need to have rules in place that give consumers the option to share their information or keep it private. Both bills before us require that companies explain to consumers what information is being collected and gives them the ability to opt out of certain data collection practices. And I think this is what consumers are looking for. They want a simple explanation followed by a choice. But there are literally thousands—millions of new businesses that have been created as a result of the ability to share information, and I think that this is absolutely vital that we protect that interest as well. Nearly all Internet businesses rely on some form of information gathering. So we want to insure that these businesses continue to grow, and flourish, but in a way that protects—that promotes transparency for the consumer.

So thank you for being here and thank you, Mr. Chairman. I yield back.

Mr. RUSH. Mr. Scalise, you are recognized for 2 minutes.

OPENING STATEMENT OF HON. STEVE SCALISE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF LOUISIANA

Mr. SCALISE. Thank you, Mr. Chairman. I want to thank you and Ranking Member Whitfield for having this hearing on the bills before us today, both focusing on consumer privacy. I am pleased that we are once again examining this issue and that legislation has been brought forward with the goal of protecting consumers and their personal information. I look forward to hearing from our panelists and discussing the merits of these bills. As we take them into consideration and debate the best steps moving forward, I hope we proceed wisely and carefully.

As I have stated at previous hearings, I hope we focus on how to protect consumers and their personal information, and look at steps the industry will take on their own to do that. We need to make sure that these bills do not focus on ways government can get involved in more areas of people's lives where it does not belong. For this reason, I hope these bills take self-regulation into account and include provisions that allow companies to continue with steps that they have already taken to protect personal information. If self-regulation is not sufficient, and if any additional privacy provisions or regulatory requirements are needed, they should be targeted, consistent, and not discriminate against any one business or industry. Congress should not pick winners and losers.

I also hope that these bills do not harm the ability to maintain or invest in their businesses. We must strike a balance that protects personal information without limiting a company's ability to do business in an honest and ethical way. Again, I will look forward to hearing from our panelists on whether they feel these bills strike that important balance.

Mr. Chairman, I also want to close by addressing the rumors that FCC Chairman Genachowski may add broadband classification to the commission's September 16 agenda. First of all, I do not believe that the FCC should reclassify broadband services or impose burdensome regulations on the Internet. And more importantly, the FCC should definitely not rush any process that gives Congress little time to react after returning from recess.

Over 8,000 pages of comments have been submitted to the FCC on this proposal, and the comment period is open until August 12. For reclassification to be on the September 16 agenda, the other commissioners would have to receive chairman's proposal by August 26, giving the commissioners 2 weeks to review the thousands of comments. Clearly we need to make sure that they have that ability to review those comments from the public. So I hope those rumors are in fact just rumors. Otherwise it would seem that the FCC intends on ignoring those 8,000 pages of comments as well as the bipartisan staff discussions that are ongoing on this issue. We must continue to pursue targeted legislation that serves the American people, not a hastened process that serves a political agenda.

Thank you, and I yield back.

Mr. RUSH. The chair recognizes now the gentleman from Georgia, Mr. Barrow, for 2 minutes.

Mr. BARROW. Thank you, Chairman, I will waive time.

Mr. RUSH. Mr. Green, you are recognized for 2 minutes.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Thank you, Mr. Chairman. Thank you Chairman Rush, and Ranking Member Whitfield. I want to thank you for raising the issue of consumer privacy and for holding this hearing today, and also Chairmen Rush and Boucher, as well as Ranking Member Stearns for introducing the bills which we examine today.

As technology continues to evolve, the privacy implications for consumers require frequent reexamination by Congress. In 2003 we passed the Canned Spam Act that countered the alarming rise of unsolicited span email messages that interfered with the use of Internet and email by in users. Today technology has continued its progress and as a result, we are once again confronted with challenges for protecting consumers and ensuring that private data is not shared without consent.

The ability to easily aggregate and share information over the Internet has provided tremendous benefits to our society and our economy, and the collection of consumer information can provide tremendous benefits to small and upstart businesses by allowing them to target customers that have tendencies to purchase individualized products or services. One problem, however, is that these are not the only ones using the data, and the ability and entire entities that sell this information to collect such a wide variety of in-

formation on individuals is extremely troubling because it allows bad actors to target vulnerable individuals based on very specific and granular data that has been collected across a number of online and offline platforms. We have laws that regulate how this information can be used by financial institutions in relating to medical record privacy, but outside these defined areas the information is largely unregulated and has the potential for being tremendously harmful to consumers.

I am pleased that our committee is confronting these challenges head on. It is important that we examine methods that introduce transparency into the system and give the consumers the ability to have control over the large scale data. Collection is currently occurring at most times without their knowledge. And I look forward to hearing the testimony from witnesses.

Mr. Chairman, I yield back.

Mr. RUSH. Mr. Latta is recognized for 2 minutes.

OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. LATTA. Thank you, Mr. Chairman, Ranking Member Whitfield. I appreciate you holding today's hearing on the important issue of protecting an individual's privacy.

Meaningful legislation to protect consumer's data is important, as there have been recently high profile incidences involving the compromising of consumer data that has increased privacy and concerns. There are many benefits that the Internet provides consumers and it is important that consumers are protected. However, as with many of the public policy issues that this Subcommittee considers, there needs to be a balance between protecting consumers and overburdening companies with regulations.

The collection of consumer information is a great benefit to companies that process transactions as well as to market their products. In addition, many of these company's products are based on information that the consumers submit to then obtain information specific to them. This personal information must be protected whether it regards personal health, employment, or any other information.

While it is important for companies to disclose their privacy practices, companies should not have to disclose the propriety practices or information for collecting this information. In moving forward on either of these pieces of legislation, we need and to ensure that by expanding the authority of a government agency that there are no unintended consequences on ecommerce. I have heard concerns, especially from small businesses, about this legislation have a chilling effect on ecommerce and curbing innovation. These small businesses are concerned that increased regulations will have negative effect on their businesses and have increased costs for them, and those that are self-employed ultimately which would then have to be borne by the consumers.

I will look forward to working—continue to work on—with the Subcommittee on this important issue relating to protecting consumer's privacy. In this time of rapidly advancing technology, we must protect personal information. I am hoping that this balance

can be achieved for all the parties involved, and with that, Mr. Chairman, I yield back. Thank you.

Mr. RUSH. The Chair recognizes Mr. Stearns for 5 minutes.

Statement of the Honorable Joe Barton
Ranking Member, Committee on Energy and Commerce
Hearing on Privacy Discussion Drafts
July 22, 2010

Thank you, Mr. Chairman.

I want to thank both Chairman Boucher and Chairman Rush for their efforts to advance the discussion on protecting consumer privacy. This is a topic several years in the making, and I suspect we may be reviewing this issue for a bit longer.

I will say that the timing of this hearing is a bit problematic. We all want to make sure we get this right, but we can only do that when both Members and stakeholders have adequate time to review what is proposed. We have not been afforded the time necessary to fully assess this latest draft before today's hearing, and Chairman Rush's bill was only released to the public on Monday. The deadline for testimony was Tuesday night, and I therefore wonder whether the comments given to us today can present a robust picture of the bills. I know everyone is in a rush to get home for August recess, but we have plenty of time left in our congressional session to schedule a hearing and allow Members, staff, and stakeholders the appropriate amount of time to fully examine such important proposals.

That said, I want to thank both Chairmen for their hard work. Both drafts provide us with a good framework for this discussion. I'm sure there are parts from both of these proposals that we will want to consider.

I continue to believe strongly that our information is our property, and we should be able to control who gets that information and what they can do with it. But I also recognize the value of this information to our economy and to businesses that provide valuable services and products that we want, often for free. Our lives would be very different if innovation were stifled, - especially in the online world, and the deregulatory approach in that space has unleashed great minds and great companies.

I will keep my comments today short because I am much more interested in what the experts before us have to say about these two drafts, as well as their thoughts and recommendations on comprehensive privacy legislation in general. In particular, I would like the witnesses to indicate whether the drafts apply their requirements to all parties in a competitively neutral fashion, and whether they address the types of issues raised by the newest data collection and use models as well as by Google's monitoring of WiFi connections and collection of user data without notice or consent.

I look forward to working with both of my friends, Mr. Boucher and Mr. Rush, as we continue our work in this area.

I yield back.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Thank you, Mr. Chairman, and like other members, I am very glad we are having the hearing on H.R. 5777, Best Practices Act, as well as the proposal drafted by Mr. Boucher, the Chairman of the Communication, Technology, and the Internet Subcommittee, the CTI Subcommittee. I was a sponsor, principal sponsor with Mr. Boucher on his bill, and so I am happy to join with him in soliciting comments as he did over the some 70 days. And as many of you perhaps know that I have had a lot of experience working on this privacy issue. It is complex, involves a broad range of interests. During my time as Chairman of this Subcommittee I introduced several privacy bills, so I understand the importance of transparency when it comes to collection, use and sharing of consumer information. Now it is my capacity as the CTI Subcommittee, I have been focusing on privacy issues and the Internet, which it becomes so ubiquitous in our everyday lives, that we have started to presume, just presume a certain level of privacy that may not actually exist, so that is why I think we should be looking at this privacy situation.

We must recognize that online advertising supports much of the commercial content, applications, and services that are available on the Internet today without charge and my colleagues, we do not want to disrupt this well-established and successful business model.

Now this bill Best Practices seeks to enhance transparency over the commercial use of personal information that provides consumers with choices about the collection, use, and disclosure of this information. I support providing consumers with choices and transparency, but we must also keep in mind that only the consumer knows how he or she feels about the information that is being collected, the parties doing the collecting and the purpose for which the information for which the information is ultimately collected. Congress cannot and should not make that decision for them.

Now I do have some concern with this Best Practices Act as currently drafted, including the overly expansive definition of covered information. The private right of action with uncapped punitive damages and the safe harbor provision which is too prescriptive and relies too heavily on the Federal Trade Commission. In order to have an effective safe harbor and privacy legislation we must craft a provision that creates the right incentives for businesses to subscribe to the very best practices with respect to the use of personal information of those consumer's standards that have been developed over time and are capable of being modified rapidly to address any new significant consumer privacy concern about businesses use of consumer's data.

I would like to work with my colleagues to develop a better self-regulatory structure that will protect consumers while creating the proper incentives for businesses to adopt and maintain the best privacy and protection standards. I obviously appreciate having these hearings. I regret though, Mr. Chairman, we are having a hearing only four days after the bill was publicly released. This is an important and complicated topic, and members, and staff, and our witnesses need more time to adequately analyze the provisions in

this legislation. It is a credit to Mr. Boucher. He released this privacy discussion draft on May 4, and he allowed ample time for comments. And if I recollect correctly, there were 70 different organizations, companies, universities, colleges, and concerned citizens that have taken the time to send their comments on this discussion draft.

So we have a—plenty of information to consider for his bill. So there is clearly a lot of interest out in privacy—out in the industry for privacy legislation. I feel that more time allowed for more robust discussion is necessary, so I hope we have that in the future. But again I appreciate your work, and the leadership on this issue, and also Mr. Boucher's hard work as I look forward to working with members of both Subcommittees as we try to find the good, equal balance of protecting consumers and allowing innovation to flourish.

I will just conclude and sort of mention which Mr. Scalise mentioned a little bit about the FCC and their haste to move the—from Title I to Title II, the Internet jurisdiction, and I would say—one thing that I would add to his comment is when we get back in September it will only be a couple of days perhaps until the FCC acts, and that is really not enough time for us to even consider what they are doing, so again, I urge as Mr. Scalise did that the FCC hold off. Thank you, Mr. Chairman.

Mr. RUSH. The Chair thanks all the members for their opening statements, the Chair really wants to reassure every member of this Subcommittee that the time to—necessary for deliberation will be forthcoming at that in no way do we expect to rush—pardon the pun—to rush towards judgment. However, we do feel as though we need to start this process in a robust way and a robust manner, and that is what was the intention of the Chairman. You know, discussion has got to end sometime and now is the time for the discussion to be ended and the work to begin.

So with that said, I want to welcome our witnesses now and I am so honored that these individuals have taken the time out from their busy schedule to come and share with this subcommittee their valuable information, insight, and their expertise on this most important matter that affects us, the American people. I want to introduce them now. From my left is Mr. David Vladeck——

Mr. VLADECK. Vladeck.

Mr. RUSH. Vladeck. He is the Director of the Bureau of Consumer Protection for the Federal Trade Commission. Seated next to Mr. Vladeck is Leslie—Ms. Leslie Harris. She is the President and CEO of the Center for Democracy and Technology. Next to Ms. Harris is Mr. David Hoffman. He is the Global Privacy Officer for the Intel Corporation. Seated next to Mr. Hoffman is Mr. Ed Mierzwinski. He is the Consumer Program Director for the U.S. Public Interest Research Group. And next to Mr. Mierzwinski is Mr. Ira Rubinstein. He is the adjunct Professor of Law in the New York School of Law. And next to Mr. Rubinstein is Mr. Jason Goldman. He is in Counsel, Technology, and E-commerce for the U.S. Chamber of Commerce. And then we have seated next to Mr. Goldman is Mr. Mike Zaneis, and Mr. Zaneis is the Vice-President of the Public Policy Interactive Advertising Bureau. Again, thank you all so very much for being present here at this hearing, and it is

the practice of this subcommittee to swear in the witnesses, and I ask each of you if you would stand and raise your right hand. There is a big panel of witnesses we got here.

[Witnesses sworn.]

Mr. RUSH. Please let the record reflect that the witnesses have all answered in the affirmative and now we will begin with testimony from our witnesses. We will begin with Mr. Vladeck. Mr. Vladeck, you are recognized for 5 minutes.

TESTIMONY OF DAVID VLADECK, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; LESLIE HARRIS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CENTER FOR DEMOCRACY AND TECHNOLOGY; DAVID HOFFMAN, GLOBAL PRIVACY OFFICER, INTEL CORPORATION; ED MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PUBLIC INTEREST RESEARCH GROUP; IRA RUBINSTEIN, ADJUNCT PROFESSOR OF LAW, NEW YORK UNIVERSITY SCHOOL OF LAW; JASON GOLDMAN, COUNSEL, TECHNOLOGY AND E-COMMERCE, U.S. CHAMBER OF COMMERCE; AND MIKE ZANEIS, VICE PRESIDENT, PUBLIC POLICY, INTERACTIVE ADVERTISING BUREAU

TESTIMONY OF DAVID VLADECK

Mr. VLADECK. Thank you very much, Chairman Rush, Member Whitfield, members of the Committee, I really appreciate the opportunity to be here today.

The Federal Trade Commission has a long track record of protecting consumer privacy. The Commission began examining online privacy in the mid-1990's. Initially the Commission's work was built on the so-called Fair Information Practice principles of notice, choice, access, and security. The Commission's efforts were widely credited with raising public awareness about privacy, prompting companies to post privacy policies online for the first time and improving companies' accountability for privacy practices.

In the early 2000's the FTC shifted its focus and targeted harmful uses of information, uses presenting risks to physical security, economic injury, or causing unwarranted intrusions. This approach was designed to protect privacy without imposing costly notice and choice requirements for all uses of information. The Commission's privacy agenda included aggressive enforcement on data security, children's privacy, spam, spyware, and unwanted telephone calls, telemarketing robocalls.

Last year the Commission announced that it was going to again re-evaluate its approach to privacy. We recognize that the traditional models governing consumer privacy have limitations. The Fair Information Practices model placed a heavy burden on consumers to read and understand complicated and lengthy privacy policies, and then make choices about the collection and use of their data. The harm-based model generally did not address concerns about having one's personal information exposed where there is no direct intangible consequence. Often, harms to consumers were addressed after they occurred.

Late last year the Commission began its re-evaluation of privacy by holding three round tables which highlighted a number of im-

portant themes. First and most urgently consumers do not understand the extent to which companies are collecting and using their personal data. This is a remark that I think many of the members echoed in their opening remarks. Second, existing privacy policies don't work as a means of communicating privacy practices to consumers, and certainly will not work well on small screen mobile devices like smart phones. Third, consumers do care about privacy and they care about privacy as a value in and of itself beyond any tangible economic harm that may be associated with it. And finally, as others have pointed out, the free flow of information does help make tremendous benefits possible, so we need to be cautious about restricting information exchanges and uses.

Recognizing many of these same issues, Chairman Rush and Chairman Boucher each have proposed legislation to advance the goal of improving privacy protection in today's commercial marketplace. We share this goal and we applaud Chairman Rush and Chairman Boucher for their leadership.

Although the Commission has not taken a position on the legislation, both proposals include a number of key policy objectives that the Commission supports.

First, both include requirements for data security for customer information, a requirement the Commission has long endorsed. Second, the Commission supports the proposal's data accuracy requirements, especially where the data will be used for decisions about a consumer's eligibility for benefits or services. Third, both proposals give the FTC limited rule making authority in the privacy area. We believe that the content, timing, and scope of privacy disclosures required by the legislation will benefit from broad stakeholder input and consumer testing which can be accomplished as part of an APA rulemaking proceeding. Finally, both proposals include innovations to simplify consumer's ability to exercise meaningful privacy choice.

If Congress enacts legislation in this area we urge it to consider some additional issues. Most importantly we think it would be useful to require short disclosures at the point of information collection and/or use and to give the FTC rulemaking authority so we can provide guidance on this requirement.

Let me share an example of why we think short and concise notices at the right moment are important. A few months ago it was reported that approximately 7,500 consumers had "sold their souls" to an online computer game retailer. To drive home the point the consumers don't read lengthy disclosures, the company provided a provision in its privacy policy that by placing an order with the company the consumer granted the company "the nontransferable option to claim for now and forever more your immortal soul". The company even went on to provide an opt-out provision for this particular soul selling clause, but not surprisingly very few consumers opted out. Now I don't believe that these consumers really meant to transfer their rights of their immortal soul to an online gaming company, and we think this illustration drives home the need for short and concise notices the consumers will read and understand at the time of data collection and use.

Another issue we would urge Congress to look at is whether the sharing of individual's data among companies affiliated through

common ownership should necessarily be exempt from consent requirements, especially where a company may share data with dozens or even hundreds of affiliate companies.

Finally we also have concerns that the safe harbor programs contained in the proposed legislation could lead to multiple consent mechanisms that may differ in important ways which could add to consumer confusion when consumers need more simplicity.

The Commission looks forward to working with Congress to resolve these issues and any others that may arise in order to accomplish our shared objective of improving consumer privacy, while at the same time promoting innovation and beneficial flows of information on the Internet. Thank you very much.

[The prepared statement of Mr. Vladeck follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Consumer Privacy

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

July 22, 2010

Chairman Rush, Ranking Member Whitfield, and members of the Committee, I am David Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on privacy.[1]

Privacy has been central to the Commission's consumer protection mission for more than a decade. Over the years, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.[2] In 2006, recognizing the increasing importance of privacy to consumers and a healthy marketplace, the FTC established the Division of Privacy and Identity Protection, which is devoted exclusively to privacy-related issues.[3]

Although the FTC's commitment to consumer privacy has remained constant, its policy approaches have evolved over time. This testimony describes the Commission's efforts to protect consumer privacy over the past two decades, including its two main policy approaches: (1) promoting the fair information practices of notice, choice, access, and security (the "FTC Fair Information Practices approach"); and (2) protecting consumers from specific and tangible privacy harms (the "harm-based approach"). It then discusses recent developments, including

---

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

[2] Information on the FTC's privacy initiatives generally may be found at http://www.ftc.gov/privacy/index.html.

[3] Prior to 2006, the Commission's Division of Financial Practices worked on privacy issues in addition to enforcing laws related to mortgage transactions, debt servicing, debt collection, fair lending, and payday lending. A different division was responsible for identity theft.

the FTC staff's Privacy Roundtables project – a major initiative to re-examine traditional approaches to privacy protection in light of new technologies and business models. It concludes by offering general comments on both Chairman Rush's and Chairman Boucher's proposed privacy legislation.

I. The FTC's Efforts to Protect Consumer Privacy

The FTC has a long track record of protecting consumer privacy. The Commission's early work on privacy issues dates back to its initial implementation in 1970 of the Fair Credit Reporting Act ("FCRA"),[4] which includes provisions to promote the accuracy of credit reporting information and protect the privacy of that information. With the emergence of the Internet and the growth of electronic commerce beginning in the mid-1990s, the FTC expanded its focus to include online privacy issues. Since then, both online and offline privacy issues have been at the forefront of the Commission's agenda, as discussed in greater detail below.

A. The FTC's Fair Information Practices Approach

Beginning in the mid-1990s, the FTC began addressing consumer concerns about the privacy of personal information provided in connection with online transactions. The Commission developed an approach by building on earlier initiatives outlining the "Fair Information Practice Principles," which embodied the important underlying concepts of transparency, consumer autonomy, and accountability.[5] In developing its approach, the FTC

---

[4] 15 U.S.C. §§ 1681e-i.

[5] This work included the Department of Health, Education, and Welfare's 1973 report, *Records, Computers, and the Rights of Citizens*, *available at* http://aspe.hhs.gov/datacncl/1973privacy/c7.htm, and the Organisation for Economic Cooperation and Development's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

reviewed a series of reports, guidelines, and model codes regarding privacy practices issued since the mid-1970s by government agencies in the United States, Canada, and Europe. From this work, the FTC identified four widely accepted principles as the basis of its own Fair Information Practices approach: (1) businesses should provide **notice** of what information they collect from consumers and how they use it; (2) consumers should be given **choices** about how information collected from them may be used; (3) consumers should be able to **access** data collected about them; and (4) businesses should take reasonable steps to ensure the **security** of the information they collect from consumers. The Commission also identified **enforcement** – the use of a reliable mechanism to impose sanctions for noncompliance with the fair information principles – as a critical component of any self-regulatory program to ensure privacy online.[6]

To evaluate industry's compliance with these principles, the Commission examined website information practices and disclosures; conducted surveys of online privacy policies, commented on self-regulatory efforts, and issued reports to Congress. In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, approximately one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security.[7] A majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to

---

[6] *See* Federal Trade Commission, Privacy Online: A Report to Congress (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23.shtm.

[7] *See* Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (May 2000) at 13-14, *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

participate fully in that marketplace.[8]

Although Congress did not pass the legislation recommended by the Commission, the Commission's efforts during this time, particularly its surveys, reports, and workshops, were widely credited with raising public awareness about privacy and leading companies to post privacy policies for the first time.[9] The Commission also encouraged self-regulatory efforts designed to benefit consumers, such as the development of best practices, improvements in privacy-enhancing technologies, and the creation of online privacy certification programs.

The Commission also brought law enforcement actions to hold companies accountable for their privacy statements and practices. In February 1999, for example, the Commission alleged that GeoCities, one of the most visited websites at the time, had misrepresented the purposes for which it was collecting personal information from both children and adults.[10] In 2000, the Commission challenged a website's attempts to sell personal customer information, despite the representation in its privacy policy that such information would never be disclosed to a third party.[11] These cases stressed the importance of keeping promises about the use of

---

[8] *Id.* at 36-38.

[9] In 1999, Congress also passed the Gramm-Leach Bliley-Act, 15 U.S.C. §§ 6821-27, requiring all financial institutions to provide notice of their data practices and choice for sharing data with third parties

[10] *In the Matter of GeoCities, Inc.*, Docket No. C-3850 (Feb. 5 1999) (consent order).

[11] *FTC v. Toysmart.com LLC*, 00-CV-11341-RGS (D. Mass. filed July 10, 2000). *See also In the Matter of Liberty Fin. Cos.*, Docket No. C-3891 (Aug. 12, 1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 10, 2000) (consent order) (alleging that online auction site obtained consumer data from competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *FTC v. Rennert,* No. CV-S-00-0861-JBR (D. Nev. July 24, 2000) (consent order) (alleging that defendants

consumer information and demonstrated the Commission's commitment to protecting online privacy.

B. The Harm-Based Approach

In the early 2000s, the FTC de-emphasized its fair information practices approach as the primary means of addressing privacy issues, and shifted its focus to a "harm-based approach" for protecting consumer privacy. The approach was designed to target harmful uses of information – those presenting risks to physical security or economic injury, or causing unwarranted intrusions in our daily lives – rather than imposing costly notice and choice for all uses of information.[12] The Commission's privacy agenda began to focus primarily on: (1) data security enforcement; (2) identity theft; (3) children's privacy; and (4) protecting consumers from spam, spyware, and telemarketing.

1. Data Security Enforcement

Maintaining and promoting data security in the private sector has been a key component of the FTC's privacy agenda. Through its substantial record of enforcement actions, the FTC has emphasized the importance of maintaining reasonable security for consumer data, so that it

---

misrepresented their security practices and how they would use consumer information); *In the Matter of Educ. Research Ctr. of Am., Inc.; Student Marketing Group, Inc.*, Docket No. C-4079 (May 6, 2003) (consent order) (alleging that personal data collected from students for educational purposes was sold to commercial marketers); *In the Matter of The Nat'l Research Ctr. for College & Univ. Admissions*, Docket No. C-4071 (Jun. 28, 2003) (consent order) (same); *In the Matter of Gateway Learning Corp.*, Docket No. C-4120 (Sept. 10, 2004) (consent order) (alleging that company rented customer information to list brokers in violation of its privacy policy); *In the Matter of Vision I Properties, LLC*, Docket No. C-4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant privacy policies).

[12] *See, e.g.*, Speech of Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Cleveland, Ohio, Oct. 4, 2001, *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm.

does not fall into the hands of identity thieves and other wrongdoers.

The FTC enforces several laws with data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act, for example, contains data security requirements for financial institutions.[13] The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[14] and imposes safe disposal obligations on entities that maintain consumer report information.[15] In addition, the Commission enforces the FTC Act's prohibition against unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.[16]

Since 2001, the Commission has used its authority under these laws to bring 28 cases alleging that businesses failed to protect consumers' personal information.[17] The FTC's early

---

[13] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[14] 15 U.S.C. § 1681e.

[15] *Id.*, § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[16] 15 U.S.C. § 45(a). *See, e.g., In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order) (alleging deception); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order) (alleging unfairness).

[17] *See In the Matter of Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order approved for public comment); *In the Matter of Dave & Buster's, Inc.*, Docket No. C-4291(Jun. 8, 2010) (consent order); *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. final order filed Mar. 15. 2010); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC

enforcement actions in this area addressed deceptive privacy statements – that is, the failure of companies to adhere to the promises they made to consumers regarding the security of their personal information.[18] Since 2005, the Commission has also alleged, in appropriate cases, that the failure to maintain reasonable security is an "unfair" practice that violates the FTC Act.[19]

These cases, against well-known companies such as Microsoft, ChoicePoint, CVS,

---

(N.D. Ga. final order filed Oct. 14, 2009); *In the Matter of James B. Nutter & Co.*, FTC Docket No. C-4258 (June 12, 2009) (consent order); *United States v. Rental Research Servs., Inc.*, No. 0:09-CV-00524 (D. Minn. final order filed Mar. 6, 2009); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. final order filed Dec. 30, 2009); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. final order Mar. 17, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. final order filed Jan. 28, 2008); *In the Matter of CVS Caremark Corp.*, Docket No. C-4259 (Jun. 18, 2009) (consent order); *In the Matter of Genica Corp.*, Docket No. C-4252 (Mar. 16, 2009) (consent order); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *In the Matter of MTS Inc.*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[18] *See In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[19] *See In the Matter of BJ's Wholesale Club, Inc.*, File No. 042 3160 (Sept. 20, 2005) (consent order).

LexisNexis, and more recently, Dave & Busters and Twitter, have involved such practices as the alleged failure to: (1) comply with posted privacy policies;[20] (2) take even the most basic steps to protect against common technology threats;[21] (3) dispose of data safely;[22] and (4) take reasonable steps to guard against sharing customer data with unauthorized third parties.[23] In each case, the Commission obtained significant relief, including requiring the companies to implement a comprehensive information security program and obtain regular third-party assessments of the effectiveness of that program.[24] In some cases, the Commission also obtained substantial monetary penalties or relief.[25] The Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to

---

[20] *See, e.g., In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In the Matter of MTS Inc.*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[21] *See, e.g., In the Matter of Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order approved for public comment); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *In the Matter of Reed Elsevier, Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order).

[22] *See, e.g., FTC v. Navone*, No. 2:08-CV-001842 (final order filed D. Nev. Dec. 30, 2009); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. final order filed Jan. 28, 2008); *In the Matter of CVS Caremark Corp.*, Docket No. C-4259 (June 18, 2009).

[23] *See, e.g., United States v. Rental Research Svcs.*, No. 09 CV 524 (D. Minn. final order filed Mar. 6, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (final order filed N.D. Ga. Oct. 14, 2009).

[24] In addition, beginning with the CVS case announced last year, the Commission has begun to challenge the reasonableness of security measures to protect *employee* data, in addition to customer data. *See, e.g., In the Matter of CVS Caremark Corp.*, Docket No. C-4259 (Jun. 18, 2009) (consent order).

[25] *See, e.g., FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. final order Dec. 29, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (final order filed N.D. Ga. Oct. 14, 2009).

accomplish this goal.[26]

2. Identity Theft

Another important part of the Commission's privacy agenda has been protecting consumers from identity theft, which victimizes millions of consumers every year. In 1998, Congress enacted the Identity Theft Assumption and Deterrence Act ("the Act"), which provided the FTC with a specific role in combating identity theft.[27] To fulfill the Act's mandate, the Commission created a telephone hotline and dedicated website to collect complaints and assist victims, through which approximately 20,000 consumers contact the FTC every week. The FTC also maintains and promotes a centralized database of victim complaints that serves as an investigative tool for over 1,700 law enforcement agencies.

The Commission also played a lead role in the President's Identity Theft Task Force ("Task Force"). The Task Force, comprised of 17 federal agencies and co-chaired by the FTC's Chairman, was established by President Bush in May 2006 to develop a comprehensive national strategy to combat identity theft.[28] In April 2007, the Task Force published its national strategy, recommending 31 initiatives to reduce the incidence and impact of identity theft.[29] The FTC, along with the other Task Force agencies, has been actively implementing these initiatives and

---

[26] Developments in state law have also played a major role in data security. The passage of state data breach notification laws beginning in 2003 required increased transparency for companies that had suffered data breaches and thus further enhanced the Commission's data security enforcement efforts. *See, e.g.,* Cal. Civ. Code §§ 1798.29, 1798.82-1789.84 (West 2003).

[27] 18 U.S.C. § 1028 note.

[28] Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2006).

[29] *See* The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

submitted a final report in September 2008.[30] Among other things, the Commission has trained victim assistance counselors, federal and state prosecutors, and law enforcement officials; developed and published an Identity Theft Victim Statement of Rights; and worked closely with the American Bar Association on a *pro bono* legal assistance program for identity theft victims.

Finally, the Commission has worked to implement the identity theft protections of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act").[31] Among other things, the FTC has acted aggressively to enforce consumers' right under the FACT Act to receive a free credit report every twelve months from each of the nationwide consumer reporting agencies, so they can spot incipient signs of identity theft. For example, the Commission has brought action against a company offering a so-called "free" credit report that was actually tied to the purchase of a credit monitoring service.[32]

3. Children's Privacy

The Commission has also undertaken an aggressive agenda to protect children's privacy. Since the enactment of the Children's Online Privacy Protection Act in 1998 ("COPPA") and its

---

[30] *See* The President's Identity Theft Task Force Report (2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

[31] Pub. L. 108-159.

[32] *FTC v. Consumerinfo.com, Inc.*, SACV05-801AHS(MLGx) (C.D. Cal. final order filed Jan. 8, 2007).

To provide further clarity to consumers, Congress recently enacted legislation requiring entities that advertise "free" credit reports to disclose that such reports are available pursuant to federal law at www.annualcreditreport.com. *See* Pub. L. 111-24, *codified at* 15 U.S.C. § 1681j(g). The FTC has promulgated a rule to implement this requirement, 16 C.F.R. § 610, and this week issued eighteen warning letters to companies alleging failures to comply with the rule.

implementing rule,[33] the FTC has brought 15 actions against website operators that collect information from children without first obtaining their parents' consent. Through these actions, the FTC has obtained more than $3.2 million in civil penalties.[34] The Commission is currently conducting a comprehensive review of its COPPA Rule in light of changing technology, such as the increased use of mobile devices to access the Internet.[35]

4. Unwarranted Intrusions

The Commission has also acted to protect consumers from unwarranted intrusions into their daily lives, particularly in the areas of unwanted telemarketing calls, spam, and spyware. Perhaps the Commission's most well-known privacy initiative is the Do Not Call Registry, which has been an unqualified success. The Commission vigorously enforces the requirements of the Registry to ensure its ongoing effectiveness. The FTC has brought 64 actions alleging violations of the Do Not Call Rule. These actions have resulted in $39.9 million in civil penalties and $17.7 million in consumer redress or disgorgement. During the past year, the Commission has filed several new actions that attack the use of harassing "robocalls" – the automated delivery of prerecorded messages – to deliver deceptive telemarketing pitches that promise consumers extended auto warranties and credit card interest rate reduction services.[36]

---

[33] 15 U.S.C. §§ 6501-6508; 16 C.F.R. Part 312.

[34] For a list of the FTC's COPPA cases, see http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

[35] In spring 2010, the FTC announced it was seeking comment on a broad array of issues as part of its review of the COPPA Rule. *See* http://www.ftc.gov/privacy/privacyinitiatives/childrens_2010rulereview.html.

[36] *See, e.g., FTC v. Asia-Pacific Telecom, Inc*, No. 10 CV 3168 (N.D. Ill., filed May 24, 2010).

In addition, since the enactment of the CAN-SPAM Act in 2003,[37] the Commission has brought dozens of law enforcement actions challenging spam, including cases involving deceptive spam, failure to honor opt-out requests, and failure to comply with requirements for adult labeling of spam messages.[38] For example, in June 2009, the FTC moved quickly to shut down a rogue Internet Service Provider ("ISP") that knowingly hosted and actively participated in the distribution of illegal spam, child pornography, and other harmful electronic content. The FTC complaint alleged that the defendant actively recruited and colluded with criminals seeking to distribute illegal, malicious, and harmful electronic content.[39] After the Commission shut down this ISP, there was a temporary 30 percent drop in spam worldwide.[40] Finally, since 2004, the Commission has brought 15 spyware cases, targeting programs foisting voluminous pop-up ads on consumers and subjecting them to nefarious programs that track their keystrokes and online activities.[41]

C. Ongoing Outreach and Policy Initiatives

While the Commission's consumer privacy models have evolved throughout the years, its activities in a number of areas have remained constant. In addition to enforcement, these include consumer and business education, research and policymaking on emerging technology

---

[37] 15 U.S.C. §§ 7701-7713.

[38] Detailed information regarding these actions is available at http://www.ftc.gov/bcp/conline/edcams/spam/press.htm.

[39] *FTC v. Pricewert, LLC*, No. 09-CV-2407 (N.D. Cal. final order issued Apr. 4, 2010).

[40] *See* Official Google Enterprise Blog, Q2 2009 Spam Trends, *available at* http://googleenterprise.blogspot.com/2009/07/q2-2009-spam-trends.html.

[41] Detailed information regarding each of these law enforcement actions is available at http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

issues, and international outreach.

1. Consumer and Business Education

The FTC has done pioneering outreach to business and consumers, particularly in the area of consumer privacy and data security. The Commission's well-known OnGuard Online website educates consumers about threats such as spyware, phishing, laptop security, and identity theft.[42] The FTC also developed a guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[43]

The FTC has also developed resources specifically for children, parents, and teachers to help kids stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[44] In less than 10 months, the Commission already has distributed more than 3.8 million copies of its *Net Cetera* brochure to schools and communities nationwide. The Commission also offers specific guidance for certain types of Internet services, including, for example, social networking and peer-to-peer file sharing.[45] In addition, the Commission recently launched Admongo.gov, a campaign to help

---

[42] *See* http://www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Línea have attracted nearly 12 million unique visits.

[43] *See Protecting Personal Information: A Guide For Business*, *available at* http://www.ftc.gov/infosecurity.

[44] *See* FTC Press Release, OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), *available at* http://www.ftc.gov/opa/2010/03/netcetera.shtm.

[45] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx.

kids better understand the ads they see online and offline.[46]

2. Research and Policymaking on Emerging Technology Issues

Over the past two decades, the Commission has hosted numerous workshops to examine the implications of new technologies on privacy, including forums on spam, spyware, radio-frequency identification (RFID), mobile marketing, contactless payment, peer-to-peer file sharing, and online behavioral advertising. These workshops often spur innovation and self-regulatory efforts. For example, the FTC has been assessing the privacy implications of online behavioral advertising for several years. In February 2009, the Commission staff released a report that set forth several principles to guide self-regulatory efforts in this area: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material retroactive changes to privacy policies; and (4) affirmative express consent for (or prohibition against) the use of sensitive data.[47] This report was the catalyst for industry to institute a number of self-regulatory advances. While these efforts are still in their developmental stages, they are encouraging. We will continue to work with industry to improve consumer control and understanding of the evolving use of online behavioral advertising.

3. International Outreach

Another major privacy priority for the FTC has been cross-border privacy and international enforcement cooperation. The Commission's efforts in this area are gaining greater

---

[46] *See* FTC Press Release, FTC Helps Prepare Kids for a World Where Advertising is Everywhere (Apr. 28, 2010), *available at* http://www.ftc.gov/opa/2010/04/admongo1.shtm.

[47] FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf..

importance with the proliferation of cross-border data flows, cloud computing, and on-demand data processing that takes place across national borders. To protect consumers in this rapidly changing environment, the FTC participates in various international policy initiatives, including those in multilateral organizations such as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation forum (APEC).

In APEC, the FTC actively promotes an initiative to establish a self-regulatory framework governing the privacy of data transfers throughout the APEC region. The FTC just announced that it was one of the first participants in the APEC cross-border Privacy Enforcement Arrangement, a multilateral cooperation network for APEC privacy enforcement authorities.

In a similar vein, earlier this year, the FTC, joined by a number of its international counterparts, launched the Global Privacy Enforcement Network, an informal initiative organized in cooperation with OECD, to strengthen cooperation in the enforcement of privacy laws.

Finally, the Commission is using its expanded powers under the U.S. SAFE WEB Act of 2006[48] to promote cooperation in cross-border law enforcement, including in the privacy area. The FTC has also brought a number of cases relating to the U.S.-EU Safe Harbor Framework, which enables U.S. companies to transfer personal data from Europe to the U.S. consistent with European privacy law.[49] For example, last fall, the Commission announced enforcement actions

---

[48] Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)).

[49] Companies self-certify to the U.S. Department of Commerce their compliance with a set of Safe Harbor privacy principles. If a company falsely claims to be part of this program, or fails to abide by its requirements, the FTC can challenge such actions under its deception

alleging that seven companies falsely claimed to be part of the Framework. The orders against six of these companies prohibit them from misrepresenting their participation in any privacy, security, or other compliance program.[50] The seventh case is still in litigation.[51]

II. Lessons Learned

Although the Commission plans to continue its ongoing enforcement, policy, and education initiatives, it recognizes that the traditional models governing consumer privacy have their limitations.

The FTC Fair Information Practices model has put too much burden on consumers to read and understand lengthy and complicated privacy policies and then make numerous choices about the collection and use of their data. Indeed, privacy policies have become complicated legal documents that often seem designed to limit companies' liability, rather than to inform consumers about their information practices.

The harm-based model has principally focused on financial or other tangible harm rather than the exposure of personal information where there is no financial or measurable consequence from that exposure.[52] Yet there are situations in which consumers do not want personal

---

authority.

[50] *See In the Matter of Directors Desk LLC*, FTC Docket No. C-4281 (Jan. 12, 2010); *In the Matter of World Innovators, Inc.*, FTC Docket No. C-4282 (Jan. 12, 2010); *In the Matter of Collectify LLC*, FTC Docket No. C-4272 (Nov. 9, 2009); *In the Matter of ExpatEdge Partners, LLC*, FTC Docket No. C-4269 (Nov. 9, 2009); *In the Matter of Onyx Graphics, Inc.*, FTC Docket No. C-4270 (Nov. 9, 2009); *In the Matter of Progressive Gaitways LLC*, FTC Docket No. C-4271 (Nov. 9, 2009).

[51] *See FTC v. Kavarni*, Civil Action No. 09-CV-5276 (C.D. Cal. filed July 31, 2009).

[52] *See* Speech of Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Cleveland, Ohio, October 4, 2001, *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm.

information to be shared even where there may be no risk of financial harm. For example, a consumer may not want information about his or her medical condition to be available to third-party marketers, even if receiving advertising based on that condition might not cause a financial harm. In addition, some have criticized the harm-based model as being inherently reactive – addressing harms to consumers after they occur, rather than taking preventative measures before the information is collected, used, or shared in ways that are contrary to consumer expectations.[53]

In addition, there are questions about whether these models can keep pace with the rapid developments in such areas as online behavioral advertising, cloud computing, mobile services, and social networking. For example, is it realistic to expect consumers to read privacy notices on their mobile devices? How can consumer harm be clearly defined in an environment where data may be used for multiple, unanticipated purposes now or in the future?

III. The FTC Privacy Roundtables

To explore the privacy challenges posed by emerging technology and business practices, the Commission announced late last year that it would examine consumer privacy in a series of public roundtables.[54] Through these roundtables, held in December 2009, and January and March 2010, the Commission obtained input from a broad array of stakeholders on existing approaches, developments in the marketplace, and potential new ideas.[55]

---

[53] *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1, 5 (2003).

[54] *See* FTC Press Release, FTC to Host Public Roundtables to Address Evolving Privacy Issues (Sept. 15, 2009), *available at* http://www.ftc.gov/opa/2009/09/privacyrt.shtm.

[55] Similar efforts are underway around the world. For example, the OECD is preparing to review its 1980 Privacy Guidelines (*see* http://www.oecd.org/document/39/0,3343,en_2649_34255_44946983_1_1_1_1,00.html); the European Commission is undertaking a review of the 1995 Data Protection Directive (*see*

The roundtables generated significant public interest. Over 200 representatives of industry, consumer groups, academia, and government agencies participated in the roundtables, and the Commission received over 100 written comments.

Several common themes emerged from these comments and the roundtable discussions. First, consumers do not understand the extent to which companies are collecting, using, aggregating, storing, and sharing their personal information. For example, as evidence of this invisible data collection and use, commenters and panelists pointed to enormous increases in data processing and storage capabilities; advances in online profiling and targeting; and the opaque business practices of data brokers, which are not understood by consumers. In addition, as commenters noted, consumers rarely realize that, when a company discloses that it shares information with affiliates, the company could have hundreds of affiliates.

Second, commenters and panelists raised concerns about the tendency for companies storing data to find new uses for that data. As a result, consumers' data may be used in ways that they never contemplated.

Third, commenters and roundtable participants pointed out that, as tools to re-identify

---

http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm); and the International Data Protection Commissioners' Conference released a set of draft privacy guidelines (*see* http://www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php). The FTC is closely following these international developments, recognizing that the market for consumer data is becoming increasingly globalized and consumer data is more easily accessed, processed, and transferred across national borders.

In addition, following the FTC roundtables, the Department of Commerce also held a workshop and issued a Notice of Inquiry on the related subject of privacy and innovation, in which the FTC has submitted a comment. *See In the Matter of Privacy and Innovation in the Information Economy*, Docket No.100402174-0175-01, Comments of the Federal Trade Commission (June 2008), *available at* http://www.ftc.gov/os/2010/06/100623ntiacomments.pdf.

supposedly anonymous information continue to evolve, the distinction between personally identifiable information ("PII") and non-PII is losing its significance. Thus, information practices and restrictions that rely on this distinction may be losing their relevance.

Fourth, commenters and roundtable participants noted the tremendous benefits from the free flow of information. Consumers receive free content and services and businesses are able to innovate and develop new services through the acquisition, exchange and use of consumer information. Commenters and participants noted that regulators should be cautious about restricting such information exchange and use, as doing so risks depriving consumers of benefits of free content and services.

Fifth, commenters and roundtable participants voiced concerns about the limitations of the FTC Fair Information Practices model. Many argued that the model places too high a burden on consumers to read and understand lengthy privacy policies and then ostensibly to exercise meaningful choices based on them. Some participants also called for the adoption of other substantive data protections – including those in earlier iterations of the Fair Information Practice Principles – that impose obligations on companies, not consumers, to protect privacy. Such participants argued that consumers should not have to choose basic privacy protections, such as not retaining data for longer than it is needed, that should be built into everyday business practices.

Sixth, many commenters called upon the Commission to support a more expansive view of privacy harms that goes beyond economic or tangible harms. There are some privacy harms, these participants argued, that pose real threats to consumers – such as exposure of information about health conditions or sexual orientation – but cannot be assigned a dollar value.

Finally, many participants highlighted industry efforts to improve transparency for

consumers about the collection and use of their information. At the same time, commenters questioned whether the tools are consistent and simple enough for consumers to embrace and use effectively.

IV. The Proposed Legislation

Chairman Rush and Chairman Boucher have each proposed legislation to advance the goal of improving privacy protections in the commercial marketplace. The Commission shares the goal of protecting consumer privacy and appreciates the opportunity to comment on the proposed legislation. Both legislative proposals include some key policy objectives that the Commission supports. For example, both proposals include requirements for reasonable data security for customer information, a measure which the Commission has long encouraged, as described above. The Commission also supports the proposals' data accuracy requirements, especially where the data will be used for decisions about consumers' eligibility for important benefits and services.

Further, both proposals give the FTC limited rulemaking authority under the Administrative Procedures Act (APA).[56] If Congress enacts privacy legislation, the Commission agrees that such legislation should provide APA rulemaking authority to the Commission. In particular, at the FTC's privacy roundtables, many stakeholders expressed concern about the significant difficulties associated with providing effective privacy disclosures. The content, timing, and scope of privacy disclosures required by the legislation would benefit from broad stakeholder input and consumer testing, which can be accomplished in an APA rulemaking.

Both proposals also include measures to simplify consumers' ability to exercise choice

---

[56] 5 U.S.C. § 552 *et seq.*

about how their data is collected and used. Simplifying choice would address concerns that consumers bear a heavy burden in having to read and understand lengthy privacy policies, and to exercise meaningful choices based on those policies. One way to simplify choice is to recognize that consumers do not need to exercise it for certain commonly accepted business practices – those that fall within reasonable consumer expectations. For example, it is unnecessary, and even distracting, to ask a consumer to consent to sharing his or her address information with a shipping company for purposes of shipping a product that the consumer has requested. By eliminating the need to exercise choice for such practices, consumers can focus on the choices that really matter to them, and on uses of data that they would not expect when they engage in a transaction.

To this end, the proposals exempt companies from having to secure consumers' consent to share their data for "operational" or "transactional" purposes, such as fulfillment. The Commission supports this general approach, especially if it allows more meaningful consent for uses of data beyond these purposes. The challenge will be to define "operational" or "transactional" purposes in a way that tracks consumers' reasonable expectations. Commission staff would be pleased to provide technical comments on these definitions.

If Congress enacts legislation in this area, the Commission urges it to consider some additional issues that are either not addressed in one or both proposals or that we recommend be modified. First, although it is important that companies make information about their privacy practices available to consumers, the Commission believes that any disclosure should emphasize important information consumers need to make choices, at a time when the consumer is making them. Short, clear disclosures could also enable consumers to compare privacy protections offered by different companies more easily and thus could promote competition among

businesses on privacy. If legislation is enacted, the Commission believes that it is important that it incorporate the need for simplified disclosures at a relevant point for consumers. FTC rulemaking authority could provide guidance for this requirement.

Second, sharing of individuals' data among companies affiliated through common ownership should not necessarily be exempt from consent requirements. As noted in the Commission's behavioral advertising report and at the Commission's roundtables, consumers often do not understand relationships between companies based on corporate control. Thus, if a company states that it does not share data with third parties, consumers may be surprised if that company shared data with dozens, or even hundreds, of affiliates.[57] The Commission suggests that any privacy legislation take this issue into consideration.

Third, the Commission has concerns about the safe harbor mechanism contained in the proposed legislation, under which the FTC could approve multiple industry-led "choice programs." One of the key themes that emerged from the privacy roundtables was the need for simplicity in the exercise of privacy choices. Creating multiple consent mechanisms that may differ in important ways risks adding to consumer confusion.

The Commission looks forward to working with Congress to address these issues and others to accomplish our shared objective of improving consumer privacy, while supporting beneficial uses of information and technological innovation.

V. Conclusion

The Commission is grateful for the opportunity to provide an overview of its activities in the privacy arena and to present these general comments on the legislative proposals. We look forward to continuing this important dialogue with Congress and this Subcommittee.

---

[57] *See* University of California at Berkeley, School of Information, KnowPrivacy, June 2009, at 28, *available at* http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

Mr. RUSH. The Chair now recognizes Ms. Harris for 5 minutes.

TESTIMONY OF LESLIE HARRIS

Ms. HARRIS. Chairman Rush, Ranking Member Whitfield, members of the Subcommittee, on behalf of CDT I thank you for the opportunity to testify today. Chairman Rush, you, Chairman Boucher, Representative Stearns have shown great leadership in putting the issue of consumer privacy legislation back on the Congressional agenda.

At a time when more and more personal information is collected, analyzed and sold, an astonishing 88 percent of Americans are concerned about their online privacy. A consumer privacy law is long overdue. Drafting a privacy law that can stand the test of time requires a careful balancing of interest. The law must provide consumers rights, it must provide meaningful obligations for companies, and at the same time it has to be flexible and high level enough to respond to the rapid changes in technology and changing business models. It needs to give companies certainty while at the same time encouraging privacy, innovation, and accountable practices, and of course, it needs strong enforcement. CTD believes the bills before the Subcommittee today include the essential building blocks for a privacy law that meets this test. Chairman Boucher's draft, the critical first steps to that end, we believe the Best Practices Act builds on that draft to significantly advance the discussion.

Let me just mention a few key points. Fair Information Practices, commonly known as FIPs, must be the foundation of any consumer privacy law. The Boucher draft provides the basic obligations in notice, and choice, and security, but as Mr. Vladeck said, that places most of the burden on the consumer to figure out notices. Best Practices goes further to a full set of substantive Fair Information Practices that place obligations on companies for things like specifying purposes, limiting data collection to those purposes, minimizing how long one retains data, paying attention to data quality, and integrity. And we think that in this complex environment all of those obligations are critical.

With respect to cope—scope, excuse me, CDT does support the application of a single baseline set of rules to be online and offline environment. We do support a robust definition of covered information and heightened protection for sensitive information, and we strongly support the special rules for covered entities, right now mainly ISPs, that collect all or substantially all of an individual's data stream. We are pleased with the innovative provision on accountability in Best Practices, which requires companies to conduct PIAs, Privacy Impact Assessments, and periodic reviews of privacy practices. American companies including my colleagues from Intel, HP, and Microsoft have been the global leaders in developing an accountable privacy culture within companies and we think this provision will broaden the culture of responsibility for all covered entities.

We also strongly support the inclusion of a safe harbor provision. Safe harbors, when they are backed up by rigorous internal compliance and some FTC supervision, can take account of differences between industries and create certainty for companies. It can encour-

age privacy innovation and reward the adoption of accountable practices.

Finally, strong enforcement must back up privacy rules, and we endorse the dual enforcement regime at the FTC and with the State Attorneys General. And we also applaud the inclusion of a strong private right of action in the Best Practices bill.

Mr. Chairman, thank you for the opportunity to testify and holding this important hearing. We intend to submit a lengthy side by side of the bills and our recommendations for moving forward, and we look forward to working with you to enact historic privacy legislation that consumers are strongly demanding and that we believe businesses need to compete in the global economy.

[The prepared statement of Ms. Harris follows:]

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Leslie Harris**
President and Chief Executive Officer
Center for Democracy & Technology

Before the House Committee on Energy and Commerce,
Subcommittee on Commerce, Trade, and Consumer Protection

THE BEST PRACTICES ACT OF 2010 AND OTHER FEDERAL PRIVACY LEGISLATION

July 22, 2010

Chairman Rush, Ranking Member Whitfield, and members of the Subcommittee:

On behalf of the Center for Democracy and Technology (CDT),[1] I thank you for the opportunity to testify today. Chairmen Rush and Boucher have shown great leadership in putting the issue of consumer privacy legislation back on the Congressional agenda. In a complex global economy, CDT believes a comprehensive set of rules for the collection and use of consumer data is long overdue.

The bills that are being discussed today provide the essential building blocks for a modern and flexible consumer privacy law based on established fair information practices that safeguard consumer privacy and encourage economic growth. Chairman Boucher's draft was a promising and important step on the road to omnibus legislation. Chairman Rush's BEST PRACTICES bill builds on that draft to significantly advance the discussion.

In my remarks today, I will comment on some of the most important building blocks drawn from these bills and offer a few suggestions for improvement. In the next week, CDT will submit a side-by-side analysis of the two bills with additional recommendations to reconcile the two into a final bill that I ask be included in the record.

I. The Need for Baseline Comprehensive Privacy Legislation

Privacy is an essential building block of trust in the digital age. But as the hearing record of both the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology, and the

[1] CDT is a non-profit public interest organization dedicated to preserving and promoting privacy, civil liberties, and other democratic values on the internet. CDT is widely recognized as a leader in the policy debate on consumer privacy, and we regularly testify before Congress on legislation and investigations touching on a wide range privacy issues.

Internet have documented, technology and market forces have created fundamental challenges to our assumptions about privacy. Massive increases in data storage and processing power have enabled diverse new business models predicated on the collection, analysis and retention of richly detailed data about consumers and their online — and offline — activities. While these new services and applications are often of great value to consumers, they also present new risks to consumer privacy. Americans turn to search engines to answer sensitive questions about their health. They use smart phone applications to pinpoint their location and obtain directions to a lawyer's or therapist's office. They shop, leaving digital traces of the book stores they browse, credit card numbers, and home and email addresses with "salesclerks" they never meet.

While few consumers fully grasp the extent of this large and growing data trade, both the hearing record and numerous independent studies show that practices such as deep packet inspection, online behavioral advertising, and the merger of online and offline consumer data into profiles undermine consumer trust, the fundamental building block of Internet use.[2] Privacy worries continue to inhibit some consumers from engaging in online shopping,[3] and are a top reason consumers decline to adopt location-based services.[4] A poll conducted by Zogby International in June 2010 found that 88% of Americans are concerned about the security and privacy of their personal information on the internet.[5]

Not only do the collection, sharing, and use of consumer data often clash with consumers' reasonable expectations of privacy, these activities are increasingly

---

[2] *See e.g.*, Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, PUBLIUS' FORUM, June 9, 2010, http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll; Joseph Turrow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf. *See also* Alan F. Westin, *Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases when Privacy Safeguards Introduced*, HARRISINTERACTIVE, April 10, 2008, http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-with-Websites-Customizing-C-2008-04.pdf (in which majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, *Use of Cloud Computing Services*, PEW INTERNET & AMERICAN LIFE PROJECT, September 2, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

[3] *See* John B. Horrigan, *Online Shopping*, PEW INTERNET & AMERICAN LIFE PROJECT, February 13, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf.

[4] Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, & Norman Sedeh, *Location-Sharing Technologies: Privacy Risks and Controls*, CYLAB USABLE PRIVACY & SECURITY LABORATORY 18 (2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[5] This poll also found that 80% of Americans are concerned about companies recording their online activities and using this data to advertise and turn a profit. *See* Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, PUBLIUS' FORUM, June 9, 2010, http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll.

outside of consumers' control. Online, even very savvy consumers are being thwarted in their efforts to take technological steps to protect their privacy and are seeing the privacy decisions they make directly overridden.[6]

The lack of consumer trust in the Internet also threatens to undermine the American economy. As the FCC wrote in the National Broadband Plan, a networked, "high-performance America" will require a policy framework that ensures the protection of consumers' privacy:

> As aspects of individuals' lives become more "digitized" and accessible through or gleaned from broadband use, the disclosure of previously private, personal information has made many Americans wary of the medium. Innovation will suffer if a lack of trust exists between users and the entities with which they interact over the Internet. Policies therefore must reflect consumers' desire to protect sensitive data and to control dissemination and use of what has become essentially their "digital identity." Ensuring customer control of personal data and digital profiles can help address privacy concerns and foster innovation.[7]

The Department of Commerce — in a recent Notice of Inquiry,[8] and the Federal Trade Commission — in a recent series of roundtables,[9] have both emphasized that privacy protections provide a foundation for e-commerce and the full realization of the potential benefits of the networked world. Yet the United States still has no comprehensive law that spells out consumers' privacy rights in the commercial marketplace. Instead, a confusing patchwork of distinct standards has developed over the years, with highly uneven results and many gaps in coverage. For example, while there is a strong privacy law for cable viewing and video records, the collection and use of purchasing data, search data, and location data held by smart phone applications are subject only to the FTC's general Section 5 authority.

---

[6] Consumers who use their browser controls to block or delete traditional tracking cookies may have their choices overridden by advertising networks that simply use a new technology, such as Flash cookies or browser fingerprinting to track their online behavior. *See* Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas & Chris Jay Hoofnagle, *Flash Cookies and Privacy*, SOCIAL SCIENCE RESEARCH NETWORK, August 10, 2009; Peter Eckersley, *How Unique is Your Web Browser?*, ELECTRONIC FRONTIER FOUNDATION, https://panopticlick.eff.org/browser-uniqueness.pdf; Wendy Davis, *ClearSight Launches Targeting Platform Tying IP Address to Offline Data*, MEDIAPOSTNEWS, June 28, 2010, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=131044.

[7] FEDERAL COMMUNCIATIONS COMMISSION, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 7-12, 52-57, http://download.broadband.gov/plan/national-broadband-plan.pdf.

[8] Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21226 (April 23, 2010).

[9] *Exploring Privacy: A Roundtable Series*, FEDERAL TRADE COMMISSION (2009-2010), http://www.ftc.gov/bcp/workshops/privacyroundtables.

For many companies, the growth of cloud computing is also bringing new urgency to the call for privacy legislation. As American companies continue to innovate and expand their markets overseas, they are finding that America's weak privacy framework is bad for business. Without adequate privacy protections in place, individuals, companies, and governments in other countries do not feel comfortable — or in many cases are legally restricted from — taking advantage of U.S.-based cloud computing services.[10] With our advanced technology and infrastructure, U.S. companies and the U.S. economy are poised to lead adoption of this hugely important new generation of cloud-based services. But to do so, Congress must move quickly to put a robust privacy framework in place.

II. Scope

CDT strongly supports the enactment of a uniform set of baseline rules for personal information collected both online and off-line. Both the Boucher draft and the Rush BEST PRACTICES bill take this comprehensive approach. Modern data flows often involve the collection and use of data derived and combined from both online and offline sources, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well. CDT also supports both bills' robust definitions of covered information, which go beyond traditional identifiers to include unique pseudonyms and persistent identifiers such as internet protocol (IP) addresses, and other information that could be reasonably be associated with an individual. The BEST PRACTICES bill currently empowers the FTC to update the definition of "sensitive information" in Section 2(8)(B). We agree with that approach and urge that the FTC also be empowered to adjust the definition of "covered information" as well to respond to technological and marketplace evolution.

CDT appreciates the heightened protections in both bills for sensitive information, including precise location information. In our comments on Chairman Boucher's draft bill, we argued for some expansion of the definition of "sensitive information," especially health information, and we think the new definitions in the BEST PRACTICES bill are close to the mark.

CDT is concerned, however, with the potential breadth of the affiliate exception in Section 2(11) of Chairman Boucher's draft bill and strongly urges that the sharing

[10] Article 25 of the EU Data Protection Directive states that the personal information of EU citizens may not be transmitted to nations outside of the EU unless those countries are deemed to have "adequate" data protection laws. The Article 29 Working Party does not consider U.S. law "adequate" (in part because the U.S. has no comprehensive data protection law), and thus in general personal information about EU data subjects may not be transferred to the U.S. for storage or other processing. While there are several compliance mechanisms, such as the U.S.-EU "Safe Harbor" agreement, that allow U.S. companies to process personal information from the EU, each comes with its own compliance challenges. For an in-depth discussion of these compliance challenges, *see Comments of the Center for Democracy and Technology on Information Privacy and Innovation in the Internet Economy*, CDT (2010), http://www.cdt.org/files/pdfs/20100613_doc_privacy_noi.pdf.

of consumer information among affiliates for advertising, marketing, and other non-operational purposes be limited to entities under common branding with the covered entity — entities that a consumer would reasonably understand to be under common control. Otherwise this exception could be used to swallow the rule. We generally support the BEST PRACTICES bill's referral of this issue to the FTC for more precise definition.

Finally, CDT is pleased to see that both bills have specific rules for covered entities that collect "all or substantially all" or certain categories of a consumer's internet activity. CDT has long been concerned about companies such as internet service providers who have the ability to monitor all of a consumers' online activity through deep packet inspection for advertising or other purposes.[11] We agree that this particularly invasive level of monitoring merits special rules, and should only be done on an opt-in, affirmative consent basis. However, we recognize that the term "all or substantially all" may not give companies sufficient clarity as to which practices are covered, nor does it prohibit narrow interpretations that would render this exception meaningless. CDT recommends that the scope of this definition be specifically referred to the FTC for further clarification.

III. Fair Information Practices

As both bills recognize, Fair Information Practices (FIPs)[12] must be the foundation of any comprehensive privacy framework. FIPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. While some have discussed moving away from FIPs in the past, new sets of protections created always revolve around the same basic eight ideas just using new terminology. The most recent government formulation of the FIPs offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation. These principles, as described by the Department of Homeland Security in 2008, include:[13]

---

[11] *See What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong., 1st Sess. (2008) (statement of Alissa Cooper, Chief Computer Scientist, Center for Democracy & Technology); *The Privacy Implications of Deep Packet Inspection: Hearing Before the Subcomm. on Commc'ns, Tech. and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong., 1st Sess. (2009) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology).

[12] The first set of FIPs was released in 1973 by the Health, Education, and Welfare Department. Since that time, various versions of the FIPs have been used by federal agencies internally and externally; each agency adopts and abides by its own set of Fair Information Principles, and these principles are reflected to some extent in the various U.S. sectoral privacy laws. FIPs additionally appear, with some variation, in many international frameworks, including the OECD guidelines of 1980, the Council of Europe data privacy convention, and the EU Data Protection Directive.

[13] U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- **Transparency.** *Entities should be transparent and provide notice to the individual regarding their collection, use, dissemination, and maintenance of information.*
- **Purpose Specification.** *Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.*
- **Use Limitation.** *Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.*
- **Data Minimization.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as is necessary to fulfill a specified purpose.*
- **Data Quality and Integrity.** *Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.*
- **Individual Participation.** *Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.*
- **Security.** *Entities should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*
- **Accountability and Auditing.** *Entities should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

While both bills make significant headway toward the integration of the Fair Information Practice principles into U.S. privacy law, the BEST PRACTICES bill intelligently incorporates much of the feedback from Chairman Boucher's draft bill and puts forward strong FIPs-based privacy protections that go beyond notice and consent to a full set of substantive privacy protections.

Transparency

Both Section 3(a)(2)(B) of Chairman Boucher's draft and Section 101 of the BEST PRACTICES bill require that covered entities entities make available detailed information about the collection, storage, and use of covered information. While the required information is important, privacy policies are notoriously difficult for consumers to understand, and striking the right balance

between readability and comprehensiveness has proven elusive. Given this challenge, we recommend that rather than mandating such detailed specific elements of notice, the FTC should be empowered to institute a rulemaking on the issue. Given the wide and ever-changing variety of mediums through which people communicate and share information, including increasingly mobile devices, we strongly support the approach of Section 102(b) of the BEST PRACTICES bill to delegate to the FTC to determine how this notice should be presented to consumers. We also support that provision's explicit direction to the FTC to develop model short form notices that companies can adapt to make notice and consent more meaningful to consumers.

Purpose Specification

CDT is pleased that both bills have strong language requiring that companies clearly specify the purposes for which they collect and use consumer information. Sections 101(3), 101(4) and 102(a) of Chairman Rush's bill require that covered entities disclose the specific purposes for which consumer data is being collected in a "concise, meaningful, timely, prominent, and easy-to-understand" fashion. Similarly, Section 3(a)(2)(B)(iv) of Chairman Boucher's bill requires notice of the specific purposes for which covered entities collect and use covered information.

Use Limitation

Neither bill explicitly states that a covered entity can only collect or use covered information for the purposes specified to the consumer. However, by mandating that covered entities affirmatively specify the purposes for which they collect or use personal information, we believe use limitation is implicitly incorporated into both bills by the sections cited above under "Purpose Specification."

CDT generally supports the provisions in both bills preventing companies from revising their privacy policies retroactively to apply to previously collected information. These provisions are consistent with the manner in which the FTC has applied its authority under Section 5 to such "material changes,"[14] but it is certainly preferable to have the principle spelled out explicitly in a privacy statute. We also endorse the provision in Section 105 in the BEST PRACTICES bill that requires covered entities to post new privacy policies for thirty days before they take effect so that consumers have ample opportunity to notice and assess the changes.[15]

[14] Consent Decree, In re Gateway Learning Corp., FTC No. C-4120 (July 7, 2004), http://www.ftc.gov/os/caselist/0423047/0423047.shtm.

[15] While CDT does not expect that ordinary consumers will be checking the privacy policies of all the websites they interact with on a monthly basis, privacy advocates do pay attention. As one telling example, last month, Apple made a change to its privacy policy regarding location tracking and behavioral targeting. Within a matter of days, bloggers and other tech writers immediately publicized the changes, to the extent that Apple eventually received a letter of inquiry from Congressmen Markey and Barton about the new policies.

Data Minimization

CDT supports the language contained in Section 303 of the BEST PRACTICES bill that sets forth appropriate and well-considered high level requirements for data minimization. Data minimization must be an obligation of all companies that collect covered information, not just for those companies that take advantage of the individually managed profile exception, as is currently the case with Chairman Boucher's draft bill. While we agree with Chairman Boucher that companies should not retain consumer data for longer than needed to fulfill the purpose for which it was collected, we are not comfortable setting a specific time limit for data retention in law as in Section 3(e)(2) of the draft bill. CDT believes that a consumer privacy law should avoid such highly prescriptive mandates, which may inadvertently freeze today's practices into law and discourage future innovation. Having said that, we also believe that Section 303 of the BEST PRACTICES bill would be improved if it specifically directed the FTC to issue regulations implementing this section. Given that the current framework has utterly failed to require or even encourage companies to adopt data minimization procedures, we believe that a direct provision requiring FTC implementation regulations is appropriate.

Data Quality and Integrity

CDT likes the broad but flexible language of both bills requiring that covered entities establish reasonable procedures to assure the accuracy of the information they collect about consumers. The only material difference between Section 201 of the BEST PRACTICES bill and Section 4(a) of Chairman Boucher's draft bill is that the former requires the FTC to issue regulations to implement and interpret this section, while the latter merely permits such regulation (through the general rulemaking powers in implementing the bill granted in Section 8(3)). Both approaches have merit. However, we believe that greater direction to covered entities would be useful to set flexible but meaningful baseline standards. We believe a directive to the FTC to adopt implementing regulations is appropriate.

Individual Participation

In general, CDT approves of the opt-out/opt-in choice framework of both bills: covered entities must offer a persistent opt-out for first-party data collection and use, and must get opt-in affirmative consent for the collection and use of sensitive information. For the sharing of covered information with third parties, as a default, covered entities must get opt-in consent, although both bills offer safe harbor provisions that allow companies to only offer an opt-out if they meet certain conditions (see *infra* Section IV, "Safe Harbor"). Obviously, "notice and choice" alone has proven insufficient to protect consumers, as that model places the entire burden for privacy protection on consumers to navigate an increasingly complex data environment. That is why a modern consumer privacy framework must incorporate all of the other FIPs in order to meet the privacy challenges posed by the vast array of 21st-century technology and business practices.

The BEST PRACTICES bill includes very detailed provisions for granting consumers access and rights of correction for covered information. While we believe these provisions to be carefully considered, we are hesitant to recommend embedding such detailed provisions into law. Instead, we suggest that the Subcommittee consider referring some or all of this section to the Federal Trade Commission for implementing regulations. To the extent the BEST PRACTICES bill exempts safe harbor participants from certain access obligations (and the Boucher draft bill requires that only safe harbor participants grant consumers access), we recommend instead that reasonable access to stored covered information be treated as a universal obligation for all companies who collect and store covered information about consumers (see *infra* Section IV, "Safe Harbor,").

Security

CDT endorses the standards set forth by Section 301 of the BEST PRACTICES bill and Section 4(b) of Chairman Boucher's bill that require covered entities to enact reasonable safeguards to protect the security of covered information. Companies should be held to an objective standard while having the freedom (and indeed, the responsibility) to innovate creatively to best protect consumers' data. If the legislation does refer the question of security to the FTC for implementing regulations, it should also include the language of Section 602(c)(3) of the BEST PRACTICES bill, which prohibits the FTC from specifically prescribing particular technologies or products in regulations for security or other components of the bill.

Accountability and Auditing

Finally, we strongly applaud the inclusion in Section 302 of the BEST PRACTICES bill of a requirement for companies to conduct Privacy Impact Assessments before collecting and using the data of large numbers of consumers, and to conduct periodic reviews of its privacy practices. American companies have played a leadership role in identifying and implementing accountable practices that safeguard privacy. In the absence of baseline privacy law, many companies have moved ahead with the appointment of privacy officers to guide internal privacy decision-making and to engage in privacy risk assessment and privacy by design.[16] And just last week the European Union's Article 29 Working Party released an opinion that was devoted entirely to an exploration of promising accountability frameworks and that recommended adoption of new accountability mechanisms by companies that handle consumer data.[17] As we noted in our comments on Chairman Boucher's draft, the inclusion

[16] For more information on how accountability measures can be incorporated into the product development cycle, *see* Marty Abrams, Ann Cavoukian, and Scott Taylor, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (Nov. 2007); http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

[17] Article 29 Working Party, "Opinion 3/2010 on the principle of accountability," 00062/10/EN WP 173 (July 2010). http://www.huntonfiles.com/files/webupload/PrivacyLaw_Accountability_WP29.pdf.

of accountability provisions in the legislation, is a way to encourage a culture of responsibility and accountability within covered entities.[18] Doing so will also support the development of a global standard on accountability.

IV. The Safe Harbor Framework

CDT strongly supports the inclusion of a safe harbor provision in the BEST PRACTICES Act. CDT has long supported the use of a flexible safe harbor framework as the most effective tool to implement the Fair Information Practice principles over a wide range of industries that collect and use personal information.[19] Given the necessary disparity in practices among varying groups such as behavioral advertisers, data brokers, small offline businesses, and multinational online retailers, a one-size-fits-all approach that narrowly prescribes all data practices is likely to unfairly favor certain industries while stifling innovation and development in others. A carefully crafted safe harbor program — backed up by a rigorous internal compliance regime — that gives industries and industry segments flexibility to develop tailored privacy solutions that are consistent will the law, is the best way to accommodate differences between industries, create certainty for companies (because following approved practices would be deemed compliance with the privacy statute), encourage privacy innovation over time, and reward the adoption of accountable practices.[20]

Finding the right balance between industry self-regulation, encouraging new technologies and business practices that protect privacy, and government oversight is obviously the key challenge in defining the parameters of a reasonable safe harbor. In designing a safe harbor, it is important to strike a balance between strong incentives to participate in a safe harbor with meaningful regulatory oversight. We believe that the BEST PRACTICES bill generally meets that test. We disagree, however with the approach of the BEST PRACTICES bill to the extent that it grants exemption from access requirements to covered entities which participate in an approved safe harbor (*see supra*, Section IV ("Individual Participation")). A safe harbor should not free participants from engaging in any particular Fair Information Practice. Rather, it should simply free them to develop alternative means to meet the requirement.

---

[18] *Comments of the Center for Democracy and Technology on the Staff Discussion Draft of Consumer Privacy Legislation*, CDT (2010), *available at* http://www.cdt.org/files/pdfs/20100604_boucher_bill.pdf.

[19] As noted by Ira Rubinstein in his comments to the Boucher draft bill, when Congress last considered online privacy legislation, several bills included provisions for a comprehensive self-regulatory safe harbor modeled on COPPA, including Rep. Markey's Electronic Privacy Bill of Rights Act of 1999 (H.R.3321, 106th Cong. § 4 (1999)); Sens. Burns and Wyden's Online Privacy Protection Act of 1999 (S. 809, 106th Cong. § 3 (1999)); Rep. Stearns' Consumer Privacy Protection Act of 2002 (H.R. 4678, 107th Cong. §106 (2002)); and Sen. Hollings' Online Personal Privacy Act (S. 2201, 107th Cong. § 203 (2002)).

[20] *See also* Letter to Chairman Rick Boucher from Professor Ira Rubinstein, June 1, 2010.

V. Enforcement

Baseline privacy legislation needs strong enforcement measures to give teeth to FIPs-based privacy protections, and the FTC does not need to go it alone. State attorney generals have brought a number of important online consumer protection cases in recent years, and they have a right and obligation to protect their citizens' interests. Therefore CDT supports the approach in both bills to give enforcement to both the Federal Trade Commission and state Attorneys General. We also support the statutory penalty provision in Section 603 of the BEST PRACTICES bill, though we believe that these penalties should be available to the Federal Trade Commission as well as the states. As we have testified previously, we believe the FTC should be empowered to sue for statutory penalties for all Section 5 violations and already operates at a disadvantage vis-à-vis state attorneys general;[21] there is no need to create a parallel FTC disadvantage for violations of privacy legislation.

CDT has long supported the inclusion of a strong private right of action in any privacy legislation. We are pleased Chairman Rush has included a private right of action in the BEST PRACTICES bill, but we think it could be strengthened by providing for liquidated damages instead of requiring that plaintiffs prove actual damages, and by extending the private right of action to all the Fair Information Practice principles, not just notice and choice.

However, CDT does not object to compliant participants in safe harbor programs from being exempted from the private right of action. Companies need to have some degree of assurance that meeting the standards approved by the FTC will insulate them from legal attack. If companies are in fact meeting those goals, they should not be subject to any legal action — either from government enforcers or private litigants.

VI. Preemption

CDT believes that preemption of state law in federal privacy law should be narrowly tailored to reach only those state laws that expressly cover the same set of covered entities and same set of requirements. Even then, CDT would only supports preemption if the federal law provides as much protection as the best state laws. CDT has previously objected to the overly broad preemption language contained in Chairman Boucher's draft bill, which arguably provides for sweeping field preemption of all state privacy laws. We are gratified that the preemption language in the BEST PRACTICES bill aligns closely with our suggested language, which we think is narrowly tailored to reach only those state laws that expressly cover the same set of covered entities, while allowing states to specify additional protections on sensitive areas such as health and financial information.

---

[21] Ari Schwartz, Testimony of Ari Schwartz before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Interstate, Trade, and Tourism, "Reauthorization of the Federal Trade Commission," September 12, 2007, www.cdt.org/privacy/20070912schwartz-testimony.pdf.

VII. Conclusion

CDT would like to thank Chairman Rush for the introduction of the BEST PRACTICES Act and for holding this important hearing. Today, we have taken an important step forward toward enactment of the baseline privacy legislation that consumers strongly support and that businesses increasingly need to compete in the global economy. We look forward to working closely with the Committee on this legislation. Thank you again for the opportunity to testify.

For more information, contact Leslie Harris, lharris@cdt.org, or Justin Brookman, justin@cdt.org at (202) 637-9800.

Mr. RUSH. The Chair recognizes Mr. Hoffman for 5 minutes.

TESTIMONY OF DAVID HOFFMAN

Mr. HOFFMAN. Mr. Chairman, Ranking Member Whitfield, and members of the Subcommittee, I am David Hoffman, Director of Security Policy and Global Privacy Officer at Intel Corporation, and I appreciate the opportunity to testify before you today.

Intel supports the Best Practices Act of 2010 and we believe that innovation requires a policy environment in which individuals feel confident that their privacy interests are protected. We thank Chairman Boucher and Ranking Member Stearns for putting forward such a thoughtful and important draft from which to work. Their bill and the Best Practices Act include many of the important concepts for a comprehensive U.S. privacy law and we strongly support Congress's efforts to legislate in this area. I congratulate you on the work you have done to protect consumer privacy and to promote continued technology innovation.

It is Intel's mission to deliver the platform in technology advancements that have become essential to the way we work and live. We see computing moving in a direction where an individual's applications and data will move as that person moves through his or her day. To manage these applications and data, the individual will use a wide assortment of digital devices including servers, laptop computers, smart phones, tablets, televisions, and handheld PCs. Thus it is necessary that individuals have trust in being able to create, process, and share all types of data, including data that may be quite sensitive such as health and financial information. The provisions in the bills we are discussing today can help provide a policy environment which creates that trust.

I would like to highlight five specific aspects of the two bills. First, we are pleased that both bills are technology neutral and give flexibility to the FTC to adapt the bill's principles to changes in the technology. Maintaining technology neutrality in the legal framework provides protection for individuals in a rapidly evolving society as the creation of legislation and regulatory requirements will invariably trail innovation of new technology. We specifically like the Best Practices Acts guidance given to for the FTC to create regulations for certain key provisions of the bill.

Second, we support federal legislation based upon the Fair Information Practices as articulated in the 1980 OECD Privacy Guidelines. We are pleased that the Boucher/Stearns discussion draft is based upon the framework of the Fair Information Practices. Further, we are supportive of Chairman Rush's bill which goes further and includes provisions applying all of the Fair Information Practices such as individual access to data, data minimization, and purpose specification.

Third, we are pleased that the Best Practices Act includes a provision requiring covered entities to engage in the accountability processes in the deployment of technologies and services. In addition we would advocate that a specific privacy by design requirement also be included in the accountability section. A privacy by design model focuses on insuring that privacy is included as a foundational component of the product and service development process. Such a provision should not require compliance with detail

standards or mandatory third party product reviews, but should instead focus on including privacy into a business's product and service development processes.

Fourth, Intel commends both bills for contemplating that certain operational uses of data are implicitly consented to by individuals and should not require explicit notice and consent. Specifically Intel supports the Best Practices Acts drafting of such a use-based model.

Fifth and finally, Intel is strongly supportive of Title IV of the Best Practices Act which establishes a safe harbor for participation and self-regulatory choice programs. Intel has long been a supporter of privacy trust mark problems and believes they provide a way to work with organizations on their accountability processes. We believe that in many instances trust marks and other similar mechanisms can substantially increase the reach and the effectiveness of government enforcement. This co-regulation is a better solution than a private right of action which is likely to result in baseless claims, causing organizations to spend resources on litigation when those resources could be better directed toward the organization's privacy compliance program. However, if a private right of action is included, then the choice program should continue to provide a safe harbor from liability.

Intel again thanks Chairman Rush and the Subcommittee for your excellent work to protect consumer privacy, and to promote and continue privacy innovation. We are supportive of the Best Practices Act, we look forward to continuing our engagement to improve the overall protection of privacy.

[The prepared statement of Mr. Hoffman follows:]

PREPARED STATEMENT OF

INTEL CORPORATION

before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

U.S. HOUSE OF REPRESENTATIVES

on

"The BEST PRACTICES Act of 2010" and other

Federal Privacy Legislation

JULY 22, 2010

I. Introduction

Mr. Chairman and Members of the Subcommittee, I am David A. Hoffman, Director of Security Policy and Global Privacy Officer of Intel Corporation. I appreciate the opportunity to appear before you today to discuss federal privacy legislation and specifically the BEST PRACTICES Act circulated by Chairman Rush and the discussion draft bill circulated by Chairman Boucher and Ranking Member Stearns.

Intel Corporation has long supported the passage of comprehensive U.S. federal privacy legislation, as we believe such legislation is foundational so that individuals can have trust and confidence in their use of technology. The two bills include many of the important concepts for a comprehensive U.S. privacy law, and we strongly support Congress' efforts to legislate in this area. I congratulate you on the work you have done to protect consumer privacy and to promote continued technological innovation. Intel thanks Chairman Boucher for putting forward such a thoughtful and important draft from which to build on, and with the minor changes discussed below, Intel supports the BEST PRACTICES Act and believes that its enactment would help further consumer privacy and the growth of the Internet.

II. Need for Federal Privacy Legislation

Intel is the leading manufacturer of computer, networking, and communications products. Intel has over 80,000 employees, operating in 300 facilities in 50 countries. In 2009 Intel had over $37 billion in revenue from sales to customers in over 120 countries. Intel develops semiconductor products for a broad range of computing applications. These products are some of the most innovative and complex products in history. For example, an Intel Core i7 processor has over 781 million transistors on each chip. It is our stated mission to serve our customers, employees, and shareholders by relentlessly delivering the platform and technology advancements that have become essential to the way we work and live. It is part of our corporate strategy to fulfill this mission by tackling big problems such as the digital divide, education, energy/environment, services, and health. However, we consistently hear that one of the barriers for using technology to address these problems is the concern that personal privacy will not be protected. Thus, Intel believes that putting in place a legal and regulatory system that provides for strong privacy protections is key to the growth of our business.

Intel currently markets and is in the process of designing a wide array of products to work on these big problems. Our core product, the microprocessor, drives computers and servers, thus directly impacting the online experience of most individuals. Intel sees computing moving in a direction where an individual's applications and data will move as that person moves through his or her day. The person will wake to having data on a certain device in his or her home, will transition to a car that has access to those applications and data, will have access at work (which often will not be in a traditional office), and then will access the data and applications after work either at home or while socializing. To manage these applications and data, the individual will use a wide assortment of digital devices including servers, laptop computers, tablets, televisions, and handheld PCs. Intel's goal is to provide the semiconductor

products that will serve as the primary computing components for those devices. It is central to our strategy that individuals will have trust in being able to create, process, and share all types of data, including data that may be quite sensitive, such as health and financial information. Intel is well on its way to innovating these future technologies. However, all of this innovation requires a policy environment in which individuals feel confident that their privacy interests are protected.

Intel is not working alone to make these innovations a reality. Companies worldwide need to be able to work with each other to bring innovative solutions to the global market. In the technology sector, it is rare when one company can work in isolation, whether they are creating hardware components, portions of the software stack, or services layered on top of the hardware and software. Companies need access to the best available people, processes and technology, to continue the innovations necessary to drive the global digital infrastructure and remain competitive in the global marketplace. Laws and regulations impacting the ability to collaborate and share information need to keep pace with our technical need for such collaboration. At the same time, and in addition to these technical preconditions, building trust in the digital economy is an essential component of driving the global digital infrastructure forward. Building a trusted environment in a systemic way not only benefits consumers and increases their trust in the use of technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth.[1] Intel strongly believes that comprehensive U.S. federal privacy legislation is a key mechanism for building this consumer trust in the Internet and ecommerce.

III. Overall Framework of the Bill

Intel is pleased that the BEST PRACTICES Act is technology neutral and gives flexibility to the FTC to adapt the bill's principles to changes in technology. Maintaining technology neutrality in the legal framework provides protection for individuals in a rapidly evolving technological society, as the creation of legislative and regulatory requirements will invariably trail innovation of new technology. Therefore, a focus on the application of principles -- neutral to the technology used -- enables a flexible, effective, and timely response.

We are supportive of providing rulemaking authority to the FTC to flesh out certain specific requirements and to adapt the bill's provisions to changes in technology. This rulemaking authority will provide flexibility for the FTC to respond to further innovation in technology and business models, and can be further enhanced by the FTC's use of workshops and enforcement guidance. Specifically, we are pleased that the BEST PRACTICES Act allows the FTC to conduct rulemakings in several sections: Section 2(8)(B) (allows the FTC to modify the definition of "sensitive information"); Section 2(10)(C) (allows the FTC to modify the definition of "third party"); Section 102(b) (allows the Commission to conduct a rulemaking on the

[1] Intel has recently released a paper outlining our vision of the Global Digital Infrastructure, "*Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy," available at* http://blogs.intel.com/policy/2010/07/intel_releases_global_digital_infrastructure_vision_paper.php.

content and delivery of notices to consumers); Section 102(d) (allows the FTC to modify the retention requirement for notices); Section 201 (allows the Commission to promulgate regulations on the accuracy of information); Section 202(j) and (k) (allow the Commission to promulgate rules on the exceptions to the right of access); Section 301 (the Commission can promulgate regulations on the Safeguards requirement); Section 404 (the Commission can approve a Choice Program); and Section 501(c)(2) (the Commission can promulgate rules regarding the reconstructing or revealing of identifiable information).

All of these issues in which Chairman Rush's bill has allowed for the possibility of FTC rulemaking are highly contextual. It is critical to note the importance of context and to allow flexibility so that the bill can continue to apply to the information necessary to create trust in the digital economy. Having this flexibility is the only way to ensure that this bill will be able to stand the test of time.[2] We also are supportive that the bill provides specific criteria that the Commission should use in making its determinations in those areas in which the FTC has been granted rulemaking authority. Only allowing the FTC to make rules that are consistent with congressional intent has worked well in other consumer protection statutes. *See, e.g,* The CAN-SPAM Act of 2003, 15 U.S.C. 7702(17)(B) ("The Commission by regulation pursuant to section 7711 of this title may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this chapter to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this chapter."). As with CAN-SPAM, Intel recommends that the FTC make certain that all regulations issued under this rulemaking authority should also be technology neutral, and that most context specific determinations are best handled by individual enforcement actions.

We also are generally supportive of the bill's enforcement structure. We are pleased that both bills provide enforcement powers to the Federal Trade Commission and state Attorneys General. However, we prefer the provisions in the draft by Chairman Boucher that do not allow for a private right of action. We believe that allowing a private right of action will create unnecessary litigation costs and uncertainty for businesses, but will not have a corresponding benefit to protecting consumer privacy. We believe that strong and consistent enforcement by the FTC and the state attorneys general is more than sufficient to ensure compliance with the statute. Further, allowing for punitive damages, as in section 604 of the BEST PRACTICES Act, only further exacerbates the difficulties present in such a scheme. However, if a private right of action is included, we recommend also including the safe harbor from liability for those organizations participating in an approved Choice Program, as provided in Section 401(3) of Chairman Rush's bill.

---

[2] For instance, we support the bill's recognition of context in the definition of "covered information." The bill rightly recognizes that whether a unique persistent identifier, such as an IP address, should be covered under the statute is dependent upon how the IP address is used and whether it can identify a specific individual.

IV. OECD Fair Information Practices

Intel supports federal legislation based on the Fair Information Practices (FIPs) as described in the 1980 Organization for Economic Co-operation and Development (OECD) Privacy Guidelines. The principles in these guidelines are as follows:

1) **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 and consent of the data subject.
2) **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.
3) **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.
4) **Use Limitation Principle** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with principle 3, above, except: (a) with the consent of the data subject, or (b) by the authority of law.
5) **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.
6) **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.
7) **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 or her; (b) To have communicated to him or her, data relating to him or her (i) 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 or her; (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/her and, if the challenge is successful to have the data erased, rectified, completed or amended.
8) **Accountability Principle** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

V. Applying the OECD Fair Information Practices to these Bills

Intel is strongly supportive of the overall framework in both of the bills, as they apply many of the OECD FIPs principles. For example, we are pleased that Chairman Boucher's discussion draft requires express affirmative consent for collecting or disclosing sensitive

information, requires reasonable procedures to assure the accuracy of covered information, and requires businesses to maintain the security of information. We are especially pleased that Chairman Rush's bill goes further and includes provisions applying all of the OECD FIPs, and we want to discuss five areas in particular.

First, we are pleased that BEST PRACTICES Act incorporates the Fair Information Practice of Individual Participation by including an explicit requirement of providing reasonable access to individuals to data that pertains to them (Section 202). Providing individuals access to data that relates to them is a necessary mechanism to building trust in the use of technology. We believe that the bill contains a reasonable approach that requires a covered entity to provide specific information (with a number of well-grounded exceptions) to individuals when the entity denies the individual a right, benefit, or privilege based upon the information. Yet when the covered entity does not deny the individual a right, benefit, or privilege, then a general notice or representative sample is all that is required. This middle-ground approach recognizes the realities of business operations, while at the same time providing strong consumer protections.[3]

Second, we are supportive of Chairman Rush's incorporation of the data minimization principle (Section 303). The large number of security breaches show us that the best way to mitigate the potential for harm to the individual is for the organization to minimize the amount of information it stores. Additionally, traditionally a data minimization provision is coupled with a collection limitation provision, which limits the amount of data to that which is necessary to fulfill the specified purpose of the data collection. We believe additional implementation of a collection limitation requirement should also be considered during discussions of the bill.

Third, we support the principle of purpose specification, which is included in Section 101(3) and (4) of the BEST PRACTICES Act. Purpose specification requires a business to look at the facts and circumstances through which the data is collected, and requires analyzing the collection from the perspective of why the individual believes he or she is providing the data. The OECD definition of Purpose Specification states that the purpose "should be specified not later than at the time of data collection." Given that privacy policies are only rarely read in detail by individuals, it is more appropriate to look to the context of the collection of the data to define the specified purpose. As smaller handheld computing devices are increasingly used over the next few years, it will be even more important to focus on the context of the collection, as the reading of lengthy privacy policies will be even more unlikely. Thus, we are also pleased that Section 102 mandates that notices must be "concise, meaningful, timely, prominent, and easy-to-understand" and that the section also takes into account that short notices may be appropriate, based upon such factors as the devices upon which notices are given.

[3] We are uncertain, however, whether it would be considered a denial of a "benefit" if a covered entity were to prohibit an individual from using a free web service based upon information that the entity possesses. However, such specific compliance questions like this could be addressed in rulemaking proceedings.

Fourth, we strongly support Chairman Rush's inclusion of the concept of accountability in Section 302 of the draft. Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation.[4] Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles that have privacy and security integrated as foundational elements. Intel and other like-minded companies are currently committing significant resources to "being accountable" in this way now, and we believe that the accountability provision is one of the more significant provisions in the draft.[5]

Finally, while some organizations may believe that the Fair Information Practices concepts do not provide them with great enough certainty to construct their compliance programs, we feel strongly that any bill must be focused on these high level principles and concepts so that it will stand the test of time in an environment where technology is rapidly evolving. And the bill's approach to allow the FTC to further define and enforce flexible requirements, while gaining the assistance of industry and consumer groups to best define enforcement guidance, is the correct approach.[6]

VI. "Use and Obligations" Model

Intel is pleased that both bills have incorporated the concepts of "operational purpose" and "service provider" and have excluded uses in those definitions from the notice and consent

---

[4] Although the definitions of accountability vary, a good approximation of the accountability concept is the following: "Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions". Center for Information Policy Leadership, submission for Galway conference convened with the OECD in Dublin, Ireland.

[5] We discuss in Section IX of the testimony how the concept of accountability can be incorporated into and further defined in a self-regulatory choice program.

[6] We would like to point out two additional provisions that might need further clarification as the legislative drafting process occurs. First, we have questions regarding the definition of "publicly available information" in Section 2(7). Under this provision, we are uncertain whether the phrase "widely distributed media" in Section 2(7)(A)(ii) would include information distributed on the Internet, including "covered information" posted by third parties. Second, we are uncertain about how an individual's revocation of consent in Section 103(c) would work in practice. That section does not state what obligations a covered entity has with regards to covered information once an individual executes a subsequent opt-out. Further, the section is silent as to a covered entity's obligations with regards to information already transferred to a third party under a covered entity's privacy policy. Operationally, it would be highly impractical to take any action regarding data already legally transferred to a third party; if the section is to contain any post opt-out obligations, it likely would have to apply only to subsequent uses by the collecting "covered entity" or transfers of data to third parties.

provisions. Intel supports what is known as a "use and obligations" model, which has been thoroughly explained in The Business Forum for Consumer Privacy's paper entitled "A Use and Obligations Approach to Protecting Privacy," *available at* *h*ttp://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf. The "use and obligations" framework states that the way an organization *uses* data determines the steps it is *obligated* to take to provide transparency and choice to the consumer, to offer access and correction when appropriate, and to determine the appropriateness of the data — with respect to its quality, currency and integrity — for its anticipated use. The model notes five categories of data use where individuals implicitly give consent to the collecting entity and service providers based on the context of the provision of their data. These five categories of data use are: (1) fulfillment; (2) internal business operations; (3) marketing; (4) fraud prevention and authentication; and (5) external, national security and legal.

We believe that Chairman Rush's "operational purpose" definition rightly covers these five categories of information and appropriately comes to the conclusion that neither notice nor choice are required for purposes such as processing a customer's transaction, website analytics, fraud prevention, complying with a court order, etc. We slightly disagree with the bill's approach on the use of data for marketing purposes, however.

The BEST PRACTICES Act excludes from the definition of "operational purpose" any data that is used for marketing or advertising (Section 2(5)(B)(i)). We believe, however, that notice and opt-out choice should not be not required for *all* marketing activities. Instead, we support The Business Forum for Consumer Privacy's model that "just-in-time" notice must be provided if the marketing initiatives would *not be expected by the consumer*. For other marketing, companies must provide an easy-to-read, discoverable privacy policy. Because we believe that reasonable consumer expectations should be the controlling factor in deciding whether notice is required, we thus support the provision in Section 2(5)(B)(ii) that excludes from the definition of "operational purpose" the use of information that would not be expected by a consumer acting reasonably under the circumstances. We believe that this concept should be guiding for both clauses in Section 2(5)(B).

VII. Privacy by Design

Over the past several years, regulators in multiple jurisdictions have called for more formalized and widespread adoption of the concept known as "Privacy by Design." Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation. The consensus view of these regulators – including the European Union's Article 29 Working Party, the FTC, and the European Data Protection Supervisor – has been that the voluntary efforts of industry to implement Privacy by Design have been insufficient.

Although Intel is pleased that Section 302 of the BEST PRACTICES Act incorporates the principle of accountability (of which Privacy by Design is one form), we believe that Section 302 should specifically include a Privacy by Design provision as well. A Privacy by Design principle

should encourage the implementation of accountability processes in the development of technologies and services. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, a Privacy by Design accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

Intel views Privacy by Design as a necessary component of our accountability mechanisms that we implement in our product and service development processes. We would encourage the Subcommittee to include a provision in the bill specifically requiring that organizations ensure that privacy is included as a principle in product and service development processes.

VIII. Self-Regulatory Choice Program

Intel strongly supports Title IV of the BEST PRACTICES Act, which establishes a safe harbor for participation in a self-regulatory choice program. Intel has long been a supporter of privacy trust mark programs, and believes they should be fostered to provide mechanisms to work with organizations on their accountability processes. In the past, I have served on both the Steering Committee for BBBOnline, and on the Board of Directors of TRUSTe (on which I was Chair of the Board's Compliance Committee). Privacy trust marks, when provided with the benefit of a safe harbor through legislation, and when assisted by robust regulatory enforcement, can be the best mechanism to make certain that companies proactively put in place the organizations, systems, tools, policies, and processes necessary to proactively respect the privacy of individuals. We believe that in many instances, this co-regulation can be more effective than government or private enforcement alone, and we are pleased that the bill will incentivize businesses to participate in strong and robust programs.

We encourage the drafters, however, to specifically link the Accountability principle found in Section 302 back to Title IV's self-regulatory choice framework, and make explicit that participants in a self-regulatory choice program must incorporate accountability concepts into their requirements. Additionally, when the FTC is devising the criteria that must be present in self-regulatory programs in order to gain approval under the statute, we encourage the Commission to look to the work currently occurring between industry, think tanks, and government representatives that is further defining the elements of an accountable organization.[7]

Further, such Choice Programs will only be effective if individuals have knowledge of the opt-out provisions of Section 403(1)(A). We thus support the consumer and business education

[7] We would specifically direct the FTC's attention to the Center for Information Policy Leadership's Galway Project, mentioned above.

campaign required under Section 702 of the BEST PRACTICES Act. The FTC conducted a highly successful education campaign to promote the National Do Not Call Registry,[8] and we are pleased to see that a similar effort would be conducted with this bill.

IX. Conclusion

Intel again thanks Chairman Rush and the Subcommittee for the opportunity to engage in this debate. We are appreciative of the considerable thought that was put into both bills, which has allowed us to have this discussion today. In addition, Intel is supportive of moving forward with the BEST PRACTICES Act, and we look forward to continuing our engagement in helping to think about ways to improve the effectiveness of the U.S. legal framework and the overall protection of privacy.

[8] See www.donotcall.gov.

Mr. RUSH. Mr. Mierzwinski, you are recognized for 5 minutes.

TESTIMONY OF ED MIERZWINSKI

Mr. MIERZWINSKI. Thank you very much. Thank you very much Chairman Rush and Ranking Member—I was trying to work my timer—this one is not working, but I will try to stick to 5 minutes. Ranking Member Whitfield, members of the Committee, I am Ed Mierzwinski. I am Consumer Program Director for the Public Interest Research Group, U.S. PIRG. My testimony as submitted includes co-signed by the Consumer Federation of America and the Center for Digital Democracy. Since then four other organizations and I will provide this for the record: Consumer Action, the Consumer Watchdog, Privacy Rights Clearinghouse, and the World Privacy Forum have also endorsed the testimony.

I want to start out with one point that is really the main point that I want to make, and that is that the current digital marketing system does not meet consumer's expectations of privacy. A recent study by two leading universities, the University of Pennsylvania and the University of California at Berkeley, found that most consumers believe that the government already protects their privacy. It does not. Instead we have a digital marketing system that I call or could call the Hoover model, and I am not talking about J. Edgar. I am talking about the vacuum cleaner. The vacuum cleaner model of collecting every bit of information, every web track that a consumer ever makes and keeping it forever is the way that companies like in their virtually unregulated digital ecosystem. And we have a system right now where the Federal Trade Commission has been hobbled for 30 or 40 years by limits on its ability to improve the rules that—and that and enforce the rules by the Maggots and Moss rulemaking that was imposed on it that this Committee tried to fix in the Wall Street Reform Act, but unfortunately the Wall Street Reform Act did not finally give the Federal Trade Commission fully capable of making authority or full aiding and abetting liability, or the full ability to impose civil penalties, and we would hope that that would be on the committees agenda to continue to try to achieve those goals.

But—so our organizations share long-standing concerns for consumer privacy and look forward to working with the Committee on these matters. And the Committee has had a long-standing history of bipartisan bases working on consumer privacy, so we are very encouraged by the work that was done first by Chairman Boucher and Ranking Member Stearns, and then by you, Chairman Rush, in putting together your thoughtful proposals.

However, our concern is that the proposals tend to graft Fair Information Practices on top of the digital ecosystem that it just won't work as well as a full Fair Information Practices based provision might work. So we are suggesting that the committee start over and among the key elements of a revised bill would be a framework focused on overall data minimization. Anyone who knows the online and offline data collection industry will tell you that the focus is on data maximization, as I said, the Hoover model. "Every move you make" as the lyrics of the Police song go could be the data collection industry's theme song as we are all being watched, compiled, analyzed, and then acted upon. While

tools involving opt-in and safe harbors for example provide greater control by a consumer, they do not constrain the dramatic and far reaching growth of online and offline data collection for personalized and innovative targeting. A vast automated and powerful data collection complex has emerged capable of generating and continually revising a profile, a consumer x-ray of our habits, interests, worries, financial status, and everything else about us. It is now being collected not just on the Internet, but also whenever we use a cell phone, or play an online game, or use any other variety of electronic gimmickry that we might be carrying around with us.

Some of the specific concerns that we have, again we think the bills are thoughtful for a start, but we would urge you to consider a few other things. First of all notice and choice are not enough. And I totally agree with the other witnesses that these bills go further than the industry preferred FIPs light of notice and choice. But we need to have a greater reliance on limiting the amount of information that is collected, used, and shared, increasing the knowledge of consumers, limiting data retention, and maximizing data minimization.

The second, self-regulation has not worked. The Federal Trade Commission under various Administrations has failed in self-regulation, as has the industry. And there are several reports that I cite in my testimony that go through the details of how first the individual references service group self-regulatory body that supposedly regulated information brokers didn't work in the 1990's, then we have the network advertising initiative didn't work, and there is an IAB provision that was started last year that we don't think has worked. So we think we need greater oversight, greater statutory protections, and we need a broader private right of action. Although the Rush bill has a narrow private right of action, we don't think enrich trial lawyers. We think private rights of action deter lawlessness and they encourage companies to comply with the law. And second, we believe that state laws should always be allowed to be stronger than federal law. If you have got a good enough federal law the states will move on and do other things. But if Congress doesn't solve the job we need the States as quick responders to new problems.

With that I will just conclude my comments and tell you that I am very pleased for our organization's want to continue to work with you to refine and enhance this legislation. Thank you.

[The prepared statement of Mr. Mierzwinski follows:]

Testimony of

Center for Digital Democracy
Consumer Federation of America
U.S. Public Interest Research Group (U.S. PIRG)

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before the Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
U.S. House of Representatives

Honorable Bobby Rush, Chairman

Legislative hearing examining H.R. ____, the "BEST PRACTICES Act," and H.R. ____, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

---

22 July 2010

Chairman Rush, Representative Radanovich and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the non-profit, non-partisan U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations, the Center for Digital Democracy and the Consumer Federation of America.[1]

Thank you for the opportunity to testify before you on the important matter of how information about consumers is collected and used by businesses in the online and offline worlds. This legislative hearing examining H.R. ____, the "BEST PRACTICES Act," and H.R. ____, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual, is very timely. Every day, the collection and use of consumer information in a virtually unregulated marketplace is exploding. New technologies allow a web of interconnected businesses -- many of which the consumer has never heard of – to assimilate and share consumer data in real-time for a variety of purposes that the consumer may be unaware of and may cause consumer harm.

In this testimony, we hope to provide background on why granting consumers greater control of their personal information is critical public policy, why holding data collectors to compliance with the Fair Information Practices matters, and how the new ecology of data collection works. We will then comment on Chairman Rush's proposal, the Best Practices Act, and on another draft bill before the full committee as circulated by members Boucher and Stearns, and how those bills approach the problem and recommendations for improvements.

Our organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. The committee has a long history of protecting consumer privacy on a bi-partisan basis, going back to its efforts to strengthen the 1999 Gramm-Leach-Bliley Financial Modernization Act (GLBA). As passed, GLBA provided for greater privacy protection in the financial marketplace and allowed states to enact stronger financial privacy laws, although the Energy and Commerce committee's laudable additional goal of requiring opt-in consent for data collection and sharing was unfortunately not achieved.[2]

SUMMARY

Consumers today are surrounded by a powerful, sophisticated and ever growing marketing "ecosystem," which collects data from and about them, offline and online, in myriad ways. Collection points include online games, mobile phones, online video, email, display ads, search, in-store transactions, and public records – all these channels are tied together increasingly in real-time updates where users can be bought and sold instantly no matter where they may be. The lesson from the financial meltdown and the new financial law should be that Congress must proactively protect consumers – not as an afterthought. Consumers throughout the country increasingly depend on digital technologies to help them address critical issues related to their finances, health, and families.

---

[1] Web addresses: U.S. PIRG (uspirg.org), Center for Digital Democracy (democraticmedia.org), Consumer Federation of America (consumerfed.org).

[2] Disclosure of Nonpublic Personal Information, Public Law 106-102, 15 U.S.C. § 801-6809, see Section 6807, Relation to State Laws, available at http://www.ftc.gov/privacy/glbact/glbsub1.htm#6807 last visited 21 July 2010) "(b) Greater protection under State law. For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter..."

Today, the public has to maneuver through a complex array of increasingly personalized interactive services, including mobile and location-based applications, online videos, and social networks, as they seek information and engage in various transactions. Digital marketing poses new challenges to consumers, since it is able to combine ongoing data collection about individuals as they interact with entertainment or other information. The emergence of mobile and location-based marketing services, which permits the tracking and targeting of an individual in a "hyper-local" geographic area, adds a new dimension to consumer protection issues online. Beyond privacy concerns from data collection, a myriad of complex techniques used to market to consumers—including online "viral" peer-to-peer social media promotions, "smart" ads that learn about an online user so its offer can be changed in real-time, and even the use of neuroscience techniques designed to deliver marketing messages directly into one's subconscious (neuromarketing)—are now regularly in use and can pose real harms.

Financial service advertisers spent some $2.8 billion last year to target U.S. consumers online—for mortgages, credit and credit cards, insurance, and loans for education. A new era in financial marketing has emerged, with consumers increasingly relying on the Internet—including mobile devices—to research and apply for loans, credit, and engage in other financial transactions. While the Internet can help inform consumer decision-making about financial products (and be tremendously convenient), it can also be a confusing—and sometimes intentionally misleading—sales medium. Few consumers are aware of how the online financial marketing system operates, including the role of data collection for targeting an individual consumer for a specific loan or financial product.

To aid in understanding the new system of behavioral targeting in the Internet, last fall our organizations, joined by other leading consumer and privacy organizations, prepared a detailed "Online Behavioral Tracking and Targeting: Legislative Primer." That primer included detailed legislative recommendations, which we incorporate by reference to this testimony.[3]

Consumers need a level playing field at least, in an era where marketers work to 'immerse" them in applications designed to even subconsciously reveal or provide valuable data. A new law is required, but one which limits overall the data that can be collected from consumers; ensures that consumers have real control when personal data is used for purposes beyond that for which they provided it; and provides for effective enforcement of consumers' rights. The US should work with the EU to develop a meaningful global framework – there is no reason why EU citizens should have greater privacy controls and rights than those in US, and since many of the companies that would be subject to US privacy law also operate on a multinational basis, it would be easier for them to comply with similar standards.

DISCUSSION AND COMPARISON OF THE APPROACHES OF THE TWO ONLINE PRIVACY BILLS BEFORE THE COMMITTEE

In general, while we respect the great deal of thoughtful work that has gone into crafting the two bills before the committee, our initial comment is that they presume the validity of the current system of data collection and are built around that presumption, rather than starting from the place that we would prefer, which is a broader Fair Information Practices-based (FIPs)

[3] The legislative primer is available at http://www.democraticmedia.org/files/privacy-legislative-primer.pdf

framework. To truly protect consumers' privacy, we need to change the paradigm to a more consumer rights-based approach, as we have done with credit reporting, for instance. Commerce will adapt and thrive based on the parameters that public policy sets for consumer privacy.

Put another way, the bills don't track well with a citizen/consumer's rights in such a FIPs framework. The bills don't address the massive growth in data collection, by requiring meaningful data minimization and limits to data retention, for example. The bills largely sanction the existing and worsening regime of ongoing collection, analysis and use of off- and online data, through the industry-preferred regime of notice and choice (not the full FIPs framework). While it is very clear that the Rush Best Practices bill makes a more substantial attempt to comply with more elements of the Fair Information Practices, neither bill is primarily based on a FIPs-framework. Instead, they tend to graft some FIPs rights for consumers and responsibilities for data collectors onto a system that is based on excessive information collection.

We continue to believe that the notice and choice model promotes bureaucracy but does not promote privacy. A privacy bill that actually creates some privacy will need to set strong rules that directly protect consumer privacy, or at least be more firmly based on the Fair Information Practices (FIPs) that have been the foundation of U.S. privacy policy for the past four decades. We believe that the bills should be restructured to follow the FIPs, in much the same way. The bills both make substantial contributions and include many concepts that privacy groups and FTC staff have concluded are key to protecting privacy.

We now will discuss key elements of the bills and make recommendations for improvements.

1) Key Definitions

Covered Information: Both bills include personal identifiers such as the Internet Protocol address in the definition of "covered information." This is crucial, because assumptions can be made about consumers and they can be treated in certain ways based on such identifiers, without the need for other personal information such as a person's name or physical address. The FTC staff report on Behavioral Advertising recognizes the risks posed by IP addresses.[4] Incorporating these findings in legislation enhances consumer protection.

Sensitive Information: The definition of "sensitive information" in the Best Practices Act is better than in Mr. Boucher's discussion draft bill because it is more expansive, especially in the areas of health and finances. For example, "sensitive information" under the Boucher bill includes "medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional." However, this would not cover situations such as when a consumer researches cancer or another disease online. As that search is not part of "medical records," the information may be collected and used to make judgments about the consumer for any purpose, including employment and insurance. Similarly, the Boucher bill includes information related to financial accounts in the definition of "sensitive information," whereas the Best Practices Act definition encompasses income, assets and liabilities, a broader range of financial information.

---

[4] FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising, 21-25, (Feb 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

We further recommend protection for the sensitive information of adolescents. Adolescents are particularly vulnerable to marketing and profiling.[5] We recommend that sensitive information include age or inferences of age, if under 18, and any information associated with a profile that has age under 18. This will provide protections for those who are marked and targeted as being adolescents.

Operational Purposes: The definition of "operational" in the Best Practices Act is also an improvement over the definition in Mr. Boucher's draft, which is much too vague.

Affiliates and Third Parties: We are pleased that the Best Practices Act takes a slightly different approach to affiliates. Instead of allowing unfettered sharing of covered or sensitive information with affiliates, as Mr. Boucher's draft would do, the Best Practices Act would not allow sharing or use of such information with affiliates if consumers are unlikely to be aware of the affiliation or would not expect that sharing or use to take place. Such affiliates are appropriately treated as Third Parties, which protects consumers better. Business reasons may dictate the presentation of different brand and corporate images to consumers. Legislation which recognizes that businesses create different consumer expectations and loyalties protects consumer expectations and creates incentives for consumers to be properly informed of how their data is shared.

2) The Opt-In and Opt-out Schemes and Exceptions in the Two Bills

We expect industry to push back hard on the very notion of opt-in consent, as (somehow) striking at the very fabric of the economy. We challenge the conventional wisdom that privacy legislation that is based on an opt-in approach is not feasible. There is absolutely no reason why an opt-in approach cannot work, and work well. It is ironic that while many in the business community profess to want to offer consumers real and meaningful control over the collection and use of their data, these same companies and associations are unwilling to provide the most effective means of control for consumers – opt-in. We heard similar objections before the wildly popular national "Do Not Call" registry was implemented, and even after when its legality was unsuccessfully challenged. We were told that it would be the end of direct marketing and that consumers would no longer be able to obtain the products and services they wanted at affordable prices. This was nonsense, as the objection to opt-in is nonsense now. Businesses will become more innovative and responsive to consumers' desires concerning the collection and use of their data if they must first ask for their express affirmative consent. There are those in the industry who have said that privacy legislation ensuring consumers have greater control over their data will actually bolster the online economy. They correctly, in our opinion, see the benefits to brands and advertisers when consumers are more confident about how their information is being treated online.[6]

We are pleased that in both bills, consumers' affirmative consent – opt-in – is required if a change in a covered entity's privacy policy means that covered or sensitive information previously collected about consumers could be used or shared in a manner not previously disclosed.

---

[5] *See* Comments of CDD, et. al., COPPA Rule Review, 40-43 (June 2010), http://www.ftc.gov/os/comments/copparulerev2010/547597-00046-54855.pdf.
[6] See http://www.digidaydaily.com/stories/the-boucher-bill-right-on-time/.

Congress should recognize that in today's data collection environment, consumers face practically insurmountable obstacles when it comes to comprehending—let alone controlling—how and why their information (including on their behaviors) is being collected, analyzed and used. Research from leading privacy academics has demonstrated that the current reliance on privacy policies, which in effect buries clear disclosure in a form of digital fine print, doesn't help inform consumers. Even if the FTC, as proposed by the bill introduced by Chairman Rush, develops a new standard for such notices, many privacy and consumer experts believe that they will do little to actually help consumers maneuver through a system purposely designed to encourage them to consent to data collection. That is why most of the leading consumer and privacy groups support an opt-in regime for the collection of information. An opt-out regime will not stem the data collection tide that threatens consumer interests

If secondary use of consumers' personal information can truly benefit them, why shouldn't covered entities be required to explain exactly how and obtain their affirmative consent? We recommend that non-sensitive information should only be allowed to be collected and used for non-operational purposes for 24 hours, after which opt-in consent would be required to continue to store and use it.

We also recommend that Congress consider mandating the creation of a "Do Not Track" registry to provide consumers with an easy-to-use, effective means of controlling the most invisible collection and use of their personal information, behavioral tracking and targeting. This is when information about their online and offline activities is used to build profiles of them for marketing and other purposes. The assumptions made about consumers through behavioral tracking may be inaccurate – who among us has not searched online for information about a friend or relative's health problems, or purchased something for another person that we would not have bought for ourselves? And some consumers may simply not want to be tracked on principle. Consumers should be able to avoid all behavioral tracking and targeting if they wish through one easy step. This would work in much the same way as the federal "Do Not Call" registry, except that instead of consumers putting their own Internet Protocol Addresses in the registry, entities that engage in behavioral tracking and targeting would submit the technical information to the registry that would enable consumers to block those activities. The FTC can consult with experts to build such a system.

But even with the required notice and opt-in, consumers may not be able to fully appreciate how information about their health, finances, race or ethnicity, sexual orientation, religious beliefs, political beliefs and data about their location might be accessed and used, for purposes they never anticipated. For instance, a consumer searching for mortgage information is unaware that she is being tracked as she searches for the best deal online and that her "profile" may contain information about her race, ethnicity, financial condition, health concerns, where she travels, and other sensitive information that can influence the kinds of offers and products that she may receive. We commend the bills for advancing safeguards related to sensitive information, although more protections are required. Many consumer and privacy groups are especially pleased that the bills declare racial/ethnic and sexual orientation related information as sensitive data. We applaud that strong safeguard as a significant advance to protect consumers and citizens from emerging new forms of racial and other types of profiling that we believe can be used to discriminate against them, including involving issues of critical importance to their welfare. We know that in particular, Chairman Rush has been publicly concerned about these issues, and we

wish to take this opportunity to also thank him for his leadership on this issue. We commend both bills for inclusion of geolocation information—a critical consumer protection advance that recognizes that in this new era of "smart" phones and what's called hyper-local targeted marketing, it is essential that such highly private information is completely under the control of the individual. As we explained in a complaint[7] filed last year at the FTC, today's mobile marketing environment combines information about one's behavior [behavioral targeting] with knowledge of a consumer's actual location. Geolocation information, including the history of where we and our families spend time, requires the highest form of consumer privacy control.

But we also strongly urge the Committee to strengthen its protections for sensitive information. As we have explained to the FTC and other federal agencies, consumers are unaware about the data collection and behavioral marketing processes that now underlie their activities involving such sensitive transactions as using the Internet to research and then pursue financial transactions, including mortgages and other forms of loans and credit. Nor are they likely to recognize that when investigating concerns about a medical issue, they can become the subject of what's called "condition targeting" by the online health marketing industry. Chairman Rush's bill correctly requires the FTC to conduct a specific rule-making on the issue of sensitive data, to potentially amplify what subjects and areas should also be included. While we greatly support this provision, we hope we can work with this committee, Chairman Boucher, and other members to strengthen the section on what should be included in this extremely critical to consumer welfare section.

We also note that storing and sharing sensitive information puts consumers at risk of identity theft and other crimes. To truly protect consumers, legislation should prohibit sensitive data from being collected or used for any purposes other than for the transactions for which they have been provided. The bill just introduced by Chairman Rush requires third parties to only use sensitive data based on affirmative opt-in consent for a specific purpose only—which we support. The use of sensitive data by first parties should be granted narrowly as well, for a limited specific purpose.

We recommend that non-sensitive information should only be allowed to be collected and used for advertising purposes for 24 hours, after which opt-in consent would be required to continue to store and use it. We believe that consumers should be given as complete control over the data collection, profiling and targeting process. Not everyone will wish to participate in so-called "Safe Harbor" approaches and other longer forms of opt-out. Data collection, profiling and targeting practices beyond an initial 24 hour period for non-sensitive information should require affirmative consent from a consumer.

---

[7] Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices, Center for Digital Democracy and U.S. PIRG January 2009, (available at http://www.democraticmedia.org/files/FTCmobile_complaint0109.pdf)

3) Access, Correction, Data Retention and Other FIPs Issues

We note that neither bill requires covered entities to limit the collection of personal information to that which is necessary for the transaction or activity in which the consumer is engaging – a fundamental element of the Fair Information Practices. This, again, is why opt-in should be the standard, not-opt-out, when information will be used for secondary purposes. There is also no limit to the amount of time that covered or sensitive information can be retained and used, beyond an 18-month retention limit for managed profiles in Mr. Boucher's bill. The Federal Trade Commission should be instructed to set reasonable retention limits.

We are pleased that the Rush Best Practices Act addresses the issue of access and correction for consumers, another important Fair Information. Legislation must ensure a consumer's right to not only access their profile and related information, but a fair process where they have the right to delete incorrect data, yet neither bill provides this protection.

We are also pleased to see the provisions in the Best Practices Act for data security and privacy risk assessments.

4) Concerns about Use of Aggregated and Re-Identified Information:

We are pleased that provisions in the bill by Chairman Rush to establish safeguards for the use of so-called re-identified data, designed to prevent the reconstructing of information on a consumer. However, in today's advanced data mining and informational targeting environment, so-called aggregate information can help provide a detailed analysis of a consumer. The FTC should be authorized to conduct a rulemaking on the appropriate use of aggregate and so-called de-identified data that would both articulate best industry practices and establish the necessary consumer privacy safeguards.

5) Use of Consumer Profiles and Discussion of Issues of Consumer Harms

Members of the data collection industry, including digital marketers, have established a far-reaching system of consumer profiling. Today, as we have discussed, so-called real-time ad auctions actually sell access to our online profiles to the highest bidder. Consumers require a system where such profiles are closely analyzed and assessed, including by regulators. The propriety of the online profiling system for consumer targeting—now across the offline and online platforms, including mobile—must be questioned. We urge the committee to require the FTC to engage in a Rulemaking on the issue of profiles and what are appropriate policies for their role. We especially suggest the FTC be mandated to examine how the use of online profiles raises consumer protection concerns in such areas as health and financial transactions a consumer makes.

6) Concerns About "Publicly Available Information"

We are concerned that this provision creates an unfortunate loophole which sanctions the collection and use of greater amounts of data on an individual consumer. As the Chairman and the committee recognize, in today's online environment information about us is often made available without the consumer realizing that it will be swept into a profile or some other form of commercial database. If we pose a picture of our friends at some celebration on our social

network, and we are toasting the birthday of a friend, should that be included in what's to be considered a database for commercial use? There should be meaningful limitations on what is considered publicly available information in this new era. The FTC should be empowered to conduct a rulemaking to set reasonable limits that will protect consumers.

7) Concerns About the Self-Regulatory Safe Harbor Scheme

We are concerned about the Rush safe harbor provision for covered entities that participate in self-regulatory programs because experience has shown that such programs have fallen far short of ensuring adequate protection for the privacy and security of consumers' personal information in the past. While that safe harbor provision – including its universal opt-out requirement -- in the Best Practices Act is more robust than the exception in Mr. Boucher's discussion draft for entities that participate in self-regulatory programs, it needs to be significantly strengthened if it is retained in the legislation. As do too many other parts of the bill, the system relies extremely heavily on FTC rulemaking and enforcement, rather than on more specific guidelines and private rights of action. Any measure that provides for FTC-approved self-regulatory programs must require the FTC to closely monitor and test those programs, rather than relying on the program operators to test and monitor themselves.

We note that evidence from the Federal Trade Commission's previous encouragement of self-regulatory schemes is not promising. As Hoofnagle,[8] (2005), notes:

> "In 2000, a 3-2 majority of the FTC formally recommended that Congress adopt legislation requiring commercial web sites and network advertising companies to comply with Fair Information Practices. However, a year later with the appointment of a new FTC Chairman, the FTC embraced self-regulation again."

He then goes on to say:

> "The overall effect of the FTC's [self-regulatory] approach has been to delay the adoption of substantive legal protection for privacy. The adherence to self-regulatory approaches, such as the Network Advertising Initiative that legitimized third-party Internet tracking and the Individual References Service Group principles that concerned sale of SSNs, allowed businesses to continue using personal information while not providing any meaningful privacy protection. Ten years later, online collection of information is more pervasive, more invasive, and just as unaccountable as ever—and increasingly, the public is anesthetized to it."

Similarly, Dixon[9] (2007) found the following, in a report on the Network Advertising Initiative (NAI):

---

[8] Hoofnagle, Chris Jay, Privacy Self Regulation: A Decade of Disappointment (January 19, 2005). Available at SSRN: http://ssrn.com/abstract=650804 or doi:10.2139/ssrn.650804

[9] Dixon, Pam, Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation, World Privacy Forum, (November 2007). Available at http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf

> The NAI has made no attempt to extend its self-regulatory structure to reflect developments in the Internet sector or in business practices. Its conception of online profiling grew rapidly stale. For example, techniques exist today for tracking of consumers that do not rely on traditional cookies. As time passed, the NAI self-regulation's effectiveness toward consumer protection became less effective or and less relevant.

We are encouraged by the efforts of the current FTC to study behavioral targeting, hold workshops and make positive recommendations.[10] Nevertheless, the FTC's historic efforts at replacing privacy protection with privacy self-regulation have not been positive. Robust rules based on Fair Information Practices are required.

8) The Bills Need Stronger Private Rights of Action

The Boucher bill (section 9) would block consumers from taking legal action to enforce their rights. As you know, federal and state agencies play important roles in protecting the public, but they cannot and do not take action to resolve every situation in which consumers' rights have been violated. It is essential for individuals to be able to enforce their privacy rights and stop egregious practices. A private right of action must be provided to help ensure a level playing field and incentivize companies to respect and protect consumers' privacy.

While the Rush bill grants very limited private rights of action for certain **willful** violations (a high standard), why not give consumers full legal rights to enforce the law?

Instead, both these bills bow to industry demands to limit consumer rights to police the marketplace. Private rights of action are not designed – as industry rhetoric would have you believe – to enrich trial lawyers. Rather, the threat of a private right of action deters unsavory practices and encourages compliance with the law. Conversely, the lack of private rights of action encourages companies to ignore the law.

The marketplace functions best when consumers, federal agencies and state attorneys general can all enforce strong laws, and states can enact stronger laws when new or local threats emerge.

9) The Bills Need Stronger State Enforcement and Less Preemption

We are very concerned about the sweeping preemption in the current draft of the Boucher/Stearns legislation. The bill preempts state or local laws or regulations that include "requirements for the collection, use, or disclosure of covered information." This is incredibly broad and could block existing or new measures on the state level to limit the use of certain types of information, such as Social Security numbers, to notify consumers of data breaches, to protect health data, and to extend other needed privacy protections to consumers.

While the Rush draft incorporates a narrower form of preemption, its provisions are still problematic. Rather than a broad preemption, we recommend that any final bill set minimum

---

[10] See, eg, Remarks of David Vladeck, Director, Bureau of Consumer Protection, Exploring Privacy: A Roundtable Series, Berkeley, CA (28 January 2010) available at http://www.ftc.gov/speeches/vladeck/100128exploringprivacy.pdf

standards for privacy protection and allow states to create stronger laws and regulations to safeguard consumer data against misuse and abuse if necessary. The stronger the final bill is, the less likely that there will be any significant gaps that states will feel compelled to fill.

We also believe that state attorneys general should always have the ability to enforce the federal law, or their state laws, and then in either state or federal court, and not be restricted to federal courts.

10) Other Concerns (Lack of A Findings Section)

We believe that there should be a strong findings section at the beginning of the bills. We urge you to carefully review our suggestions, as we are working toward the same goal: to protect the interests of Americans while maintaining and increasing robust commerce. In fact, providing meaningful protection for consumers' data is necessary in order to ensure their confidence in our increasingly complex marketplace. The argument that we must choose between privacy or access to a broad array of reasonably attainable goods and services is false. American business can deliver both, and we should demand no less.

CONCLUSION

We commend Chairmen Rush and Boucher, along with Ranking Member Stearns (and other members of the committee), for helping advance a much needed legislative debate about the best way to protect consumer privacy. Consumer and privacy groups recognize the important role that online marketing and advertising play, as a source of revenues for online and other publishing, and as a robust sector of the digital economy. We also recognize that data collection, online and offline, plays an important role—perhaps the most critical one---for the industry's future.

But contemporary data collection practices, especially online, far surpass what consumers may have become familiar with on a day-to-day basis. Not only are our behaviors online closely tracked and analyzed (such as the content we like or tend to avoid; what we are willing to pay for or what we discard from online shopping carts), but consumers are confronted with an array of interactive ads purposely designed to elicit, sometimes subconsciously, greater amounts of our data. Today, as U.S. PIRG, Center for Digital Democracy and others recently filed at the FTC, so-called real-time ad exchanges auction consumers off to the highest bidder, so that they can be targeted for marketing wherever they might happen to be online. All this is done in a non-transparent, unaccountable manner, without the consumers' knowledge or consent.

A vast, automated, and powerful data collection complex has emerged, capable of generating and continually revising a profile—a consumer X-Ray—of our habits, interests, worries, financial status, families. These applications can hone in on an individual consumer, and almost instantly create an interactive ad that continues to transform itself as it stealthily "learns" about the interests of a single consumer. Google's recent acquisition of Teracent, one of the companies focused on so-called "Smart" ads, is just one example of why online marketing's ability to encourage a consumer to provide data demands a rigorous framework to protect consumer privacy. As the company explains, "Teracent deploys an unlimited number of ad creative combinations (using your catalogs, databases, images, and messages) through a single ad unit. Then, sophisticated machine learning algorithms instantly select the optimal creative elements

for each ad impression – based upon a real-time analysis of which items will convert from impressions into sales."[11]

We firmly believe that the U.S. should be the global leader in creating a policy framework shaped by FIPs that greatly aids the growth of the digital marketing industry. While advances in so-called computational advertising reflect an important contribution to innovation and can help spur the growth of ad revenues, they must be guided by a framework grounded in the requirements of consumer protection in a democratic society. That's why we—consumer and privacy groups and other concerned citizens—want to work with Chairman Rush, Chairman Boucher, Ranking Members Stearns and Radanovich—as well as Chairman Waxman and Ranking Member Joe Barton, Mr. Markey and others—to build up these initial proposals, and to work with industry, academic experts, and other stakeholders to develop legislation that is grounded in Fair Information Practices.

Among the key elements of a revised bill is a framework focused on overall data minimization. Today, anyone who knows the online and offline data collection industry will tell you the focus is on data maximization. "Every move you make," as the lyrics of the Police song go, could be the data collection industry theme song, as we are all being watched, compiled, analyzed and then acted upon. While tools involving opt-in and safe harbors, for example, provide greater control by a consumer, they do not constrain the dramatic and far-reaching growth of online and offline data collection for personalized and interactive targeting. Although the bill offered by Chairman Rush incorporates a key section on data minimization, we believe that the overall legislation should focus on mandating that less data be collected wherever possible. The online and data collection industry should not be permitted to engage, as they are, in an unchecked data "arms race." Digital data détente is required, with a system based on minimal data collection, complete transparency, consumer control and redress, and federal, state and private rights of enforcement.

OTHER BACKGROUND SECTIONS

Attachments:
Appendix 1: The Need For Privacy Protection To Be Based On The Fair Information Practices (Page 12)
Appendix 2: Interactive Advertising Data Collection Examples (3 pages, Pages 13-15)
Appendix 3: A Marketer's Guide to Understanding the Economics of Digital...2009, AAAA. (Page 16).

[11] Teracent, "Advertiser Solutions," http://www.teracent.com/advertiser-solutions/ (viewed 20 July 2010).

Appendix 1: The Need For Privacy Protection To Be Based On The Fair Information Practices

In 1973, a task force was formed at the U.S. Dept. of Health, Education and Welfare (HEW) to look at the impact of computerization on medical records privacy. The members wanted to develop policies that would allow the benefits of computerization to go forward, but at the same time provide safeguards for personal privacy.

The task force developed a Code of Fair Information Practices, consisting of five clauses: openness, disclosure, secondary use, correction, and security. At the same time, Sweden enacted a law that codified many of the same fair information principles formulated by the HEW.

In the ensuing years, other European countries enacted similar omnibus data protection laws. And in 1980, the Organization of Economic Cooperation and Development (OECD), an international body based in Paris, adopted the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."

In general, consumer and privacy organizations consider the OECD Guidelines to be the most robust version of the Fair Information Practices. Many industry self-regulatory organizations have adopted notice and choice regimes that, at best, amount to "FIPs-Lite" and at worst to bureaucracy without privacy protection. For the record, the OECD Guidelines are listed below.

Privacy Guidelines
Organization of Economic Cooperation and Development, 1980

From "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, 1980.[12]

Collection Limitation. 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. 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 Paragraph 9 [Purpose specification] 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 about 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
1. within a reasonable time; 2. at a charge, if any, that is not excessive; 3. in a reasonable manner; and 4. 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.

---

[12] Available at http://bit.ly/coc5sq (last visited 10 July 2010).

Appendix 2: Interactive Advertising Data Collection Examples[13]

1. Consumer tracking online:
As Yahoo's online ad auction service Right Media explains in a "primer" for data providers: "Data providers are changing the advertising landscape by focusing on who sees ads rather than where ads appear. Here is how it works: When consumers go to certain web sites, the page places a tag (or 'cookie') within the browser—tracking that a particular browser visited a particular site. In some cases, a data provider (which can also be described as a data 'collector') pays the web site for the ability to do this. The cookie enables the data provider to follow consumers and track their online 'behavior.'"

2. *New York Times* description of real-time ad-bidding process:
"Now, companies like Google, Yahoo and Microsoft let advertisers buy ads in the milliseconds between the time someone enters a site's Web address and the moment the page appears. The technology, called real-time bidding, allows advertisers to examine site visitors one by one and bid to serve them ads almost instantly.... Using data providers like BlueKai or eXelate, AppNexus can add information about what a person has been doing online. 'It's a lot about being able to get the right users, but it's also about passing on certain instances where we don't think you're in the market, based on what you've been doing in the past hour,' Mr. Ackley [vice president for Internet marketing and advertising at eBay] said.... Until the arrival of real-time bidding, said Mr. Mohan of Google, 'the technology hasn't really been there to deliver on the promise of precise optimization, delivering the right message to the right audience at the right time' in the display world."

3. Online tracking now combined with offline databases to create detailed profiles:
"Digital-marketing companies are rapidly moving to blend information about consumers' Web-surfing behavior with reams of other personal data available offline, seeking to make it easier for online advertisers to reach their target audiences.... eXelate will tie its data on more than 150 million Internet users to Nielsen's database, which includes information on 115 million American households, to provide more-detailed profiles of consumers. 'We can build [consumer] profiles from any building blocks,' says Meir Zohar, chief executive of eXelate.... 'Age, gender, purchase intent, interests, parents, bargain shoppers—you can assemble anything.'" eXelate "gathers online consumer data through deals with hundreds of Web sites. The firm determines a consumer's age, sex, ethnicity, marital status and profession by scouring Web-site registration data. It pinpoints, for example, which consumers are in the market to buy a car or are fitness buffs, based on their Internet searches and the sites they frequent. It gathers and stores the information using tracking cookies, or small strings of data that are placed on the hard drive of a consumer's computer when that consumer visits a participating site. Advertisers, in turn,

---

[13] These examples are derived from Center for Digital Democracy, U.S. PIRG et al complaints to the Federal Trade Commission on Online Marketing. See April 2010, Complaint - Real-time Targeting & Auctioning, Data Profiling, Optimization, And Economic Loss To Consumers & Privacy (available at http://www.democraticmedia.org/files/u1/20100407-FTCfiling.pdf) and also January 2009, Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices (available at http://www.democraticmedia.org/files/FTCmobile_complaint0109.pdf) for our most recent filings.

purchase cookie data from eXelate and use it to buy targeted online ads." eXelate's recent agreement with Nielsen will "will allow advertisers to go to eXelate to buy New York-based Nielsen's trove of data converted to a cookie-based digital format. That data comes from sources including the Census Bureau, the firm's own research and that of other consumer-research firms, such as Mediamark Research and Experian Simmons."

4. Ad exchange targeting involves such sensitive areas as health and finance:
Google's DoubleClick Ad Exchange permits the targeting of a wide range of health and financial behaviors. These include arthritis, diabetes, GERD and digestive disorders, migraines, sleep disorders, pain management, credit cards, loans and insurance.

5. Social Media marketing includes online discussions of personal health:
Social media marketing is a recent form of interactive advertising that takes advantage of a person's social relationships online—their so-called social graph—with brands and other advertising. Through various techniques and technologies, companies monitor consumer conversations about a product or medical condition, often covertly. Heartbeat Digital's BuzzScape, for example, "allows clients to monitor discussions that flow in and out of the tens of thousands of message boards, forums, blogs and social networks that increasingly dominate the online environment. 'We translate 'buzz' into ROI,' said Bill Drummy, chairman and CEO of Heartbeat. 'In a sense, we eavesdrop on public conversations among people with a shared interest, then use what we learn to create interactive marketing campaigns that address the identified needs, wants and gaps in knowledge of target audiences.'"

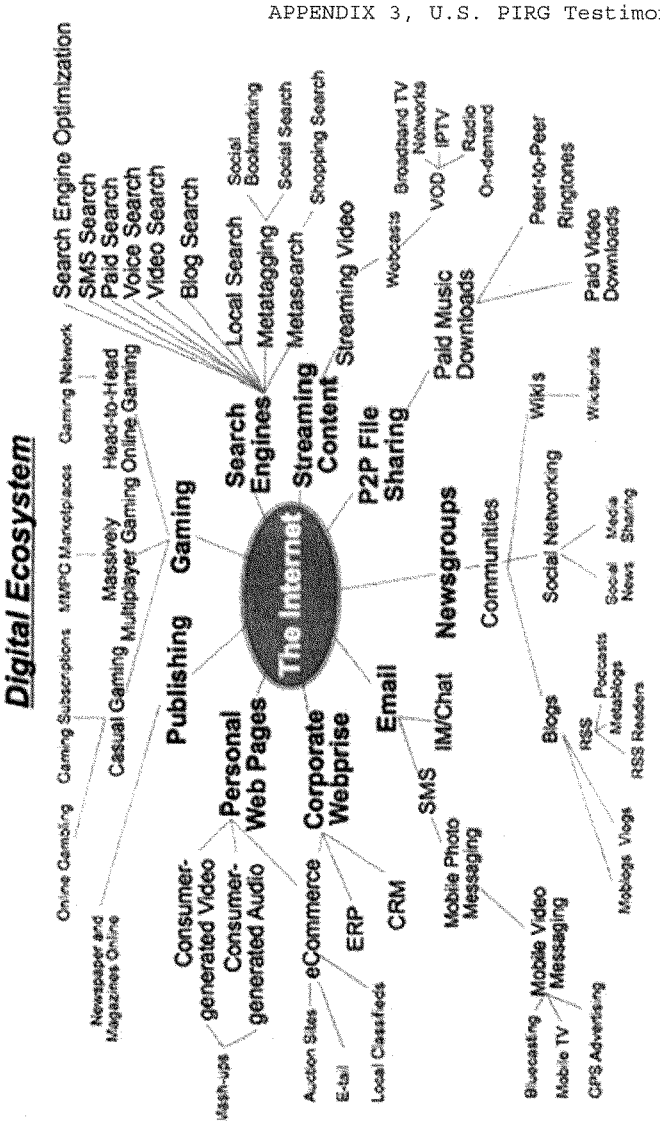
6. Even on so-called "opt-in" sites that require registration, consumers may not be fully aware of the amount and range of personal information that they are sharing with third parties:
PatientsLikeMe offers a new service, PatientsLikeMeListen, to its industry partners. In addition to giving pharmaceutical companies "unprecedented insight on how your brand is perceived," the monitoring service also provides startling amounts of personal data about the online conversants, including gender, age, time on treatment, time since diagnosis, disease progression, disease type, symptomology, longitudinal variation, and supporting therapies. As Razorfish's Debrianna Obara explains, "Sites such as Yahoo!, EverydayHealth and MSN are able to segment their audience differently. Since most of their users have created accurate profiles of themselves when they register with a site (including birth year, number of children in household, zip code, and ailments in the household), these sites can create packages for advertisers comprised only of people that fit the desired audience profile.

7. Mobile marketing poses new threats to consumer privacy:
Mobile devices, which know our location and other intimate details of our lives, are being turned into portable behavioral tracking and targeting tools that consumers unwittingly take with them wherever they go. Bango's Sarah Keefe notes how online marketers will be able to update profile-based mobile targeting in real time: "Marketers can…compile an accurate and rich understanding of their target consumer's profile. With this data jackpot, marketers can target messages to the right audience in the right geographic location. Also, real time data allows campaigns to be tweaked and refined to ensure success and optimize the marketing investment…. It's a brave new mobile marketing world out there and the wealth of data and analytics capabilities that are part of the new landscape eliminate the risk of jumping right in. Why wait?" As Mobixel reveals in its product literature, "the opportunity to reach a large

captive audience" through mobile advertising is "extremely enticing," because "the mobile phone offers focused demographic, behavioral and contextual targeting and immediate engagement." Using these capabilities, its Mobixel Ad-It service provides the tools for mobile network operators to "gather, quantify and analyze" a wide range of information about subscribers, including "demographic details, service profiles, behavioral patterns, as well as the real-time context of services, location and device and network capabilities.... It then uses this information, in real time, to make complex targeting decisions" on behalf of advertisers.

8. Location-based targeting adds a new threat to consumer privacy:
If behavioral targeting is a potent force in interactive advertising, the mobile marketplace increases the power of such targeting still further by pinpointing the precise location where various consumer behaviors take place. In the past, of course, marketers could determine the approximate location of mobile device users through a complex system of triangulation. But the latest generation of cellular phones, which are increasingly equipped with sophisticated global positioning capabilities, are taking all of the guesswork out of location-based targeting. Utilizing these advances in GPS technology, marketers can now determine the precise location of mobile users—within three feet. As Ad Age noted, "Context-based banner ads now morph into GPS locators for the closest product from the user's current location. Ads can initiate calls or purchase DVDs for instant viewing. Ads can incorporate audio, video and web browsing, and can also direct users to the iPhone App Store or iTunes."

9. Online "lead generation" in financial services:
The role of online lead generation (so-called "trigger leads") and the use of behavioral targeting for mortgages and other loans represent a potentially critical threat to the privacy of digital consumers, whose data are used without their clear understanding, let alone control, of such surveillance. For example, Lightspeed Research promises marketers a "full wallet view across customers' many financial services relationships," providing "unparalleled insight into consumers' use of credit, debit, banking and alternative payment products. We passively gather information from their financial accounts and merge it with third-party behavioral datasets, survey-based attitudinal insights, and industry expertise."



Source: *A Marketer's Guide to Understanding the Economics of Digital*.....2009, AAAA.

Mr. RUSH. Thank you. Mr. Rubinstein, you are recognized for 5 minutes.

TESTIMONY OF IRA RUBINSTEIN

Mr. RUBINSTEIN. Mr. Chairman, Ranking Member Whitfield, and members of the Subcommittee, thank you for the opportunity to testify today. My name is Ira Rubinstein and I am an adjunct professor at NYU School of Law. This afternoon I will focus my comments specifically on a key question in Congressional efforts to regulate privacy. What is the relationship between privacy legislation and industry self-regulation and the role and effectiveness of safe harbor provisions in promoting self-regulation?

A safe harbor is a familiar legislative device intended to shield or reward firms if they engage in desirable behavior as defined by statute. In the privacy arena the most familiar example is the Children's Online Privacy Protection Act. Over the past decade COPPA safe harbor programs have met with success mainly in terms of complimenting FTC's own enforcement efforts. But the program has two main shortcomings, weak incentives, and a low rate of participation. Only about 100 firms have joined. In my written testimony I propose several ways in which Congress might improve upon the COPPA safe harbor by adopting a more co-regulatory approach in which industry enjoys greater scope in shaping self-regulatory guidelines while government sets default requirements and retains general oversight authority to improve—approve and enforce such guidelines.

A co-regulatory approach relies on both sticks and carrots as incentives. Sticks for non-participating firms might include a private right of action, broader opt-in requirements, external and independent audits of regulatory compliance and much stricter requirements for online behavioral advertising. Carrots, on the other hand, might include not only exemptions from private actions for safe harbor participants, but also cost saving such as compliance reviews based on self-assessments rather than external audits, government recognition of better performing firms, and regulatory flexibility in the form of tailored requirements addressed to specific sectors or business models.

In proposing this new approach to privacy safe harbors it bears emphasizing that safe harbor benefits should be limited to firms demonstrating superior performance and would not be available to other firms that merely satisfy the fault statutory requirements. In other words, the safe harbor would only benefit firms that meet high performance standards based on, for example, sound data governance practices such as appointing a chief privacy officer who is accountable for setting privacy protection policy and standards; advanced privacy methodologies such as use of development guidelines for building privacy protection into products or services, also called privacy by design as Mr. Hoffman mentioned; and other Best Practices such as privacy training for relevant staff and online guidance on privacy and security for other employees and for consumers.

In closing I want to emphasize that this new approach to privacy safe harbor should not be confused with existing self-regulatory schemes in which industry alone develops and then oversees the

privacy code of conduct. Rather, in a privacy safe harbor as envisioned here, the government sets default requirements and relevant standards and practices emerge from a multi-stakeholder process in which both advocacy groups and members of the public have an opportunity to participate. This requires that interested parties engage in difficult and perhaps protracted negotiations and keep talking with each other until they forge a rough consensus.

One way to insure public participation is negotiated rule making, a statutorily defined process by which agencies formally negotiate rules with regulated industries and other stakeholders as an alternative to conventional rule making. An alternative approach would be to modify the safe harbor approval process by requiring that program sponsors engage in a public consultation and report on these consultations in their applications.

I will conclude by offering three recommendations which I am happy to elaborate upon during this hearing. First, Congress needs to enact comprehensive privacy legislation incorporating robust Fair Information Practices. Second, this legislation should include a safe harbor program based on a co-regulatory approach as described above. Finally, this safe harbor program should include strong performance standards based on data governance, advance privacy methodologies, and other Best Practices, and it should also require public consultation as part of the safe harbor approval process.

The two bills being considered today represent important first steps in developing this new approach to safe harbors, but should be expanded as discussed above. I want to thank you again for this opportunity to testify. I will be pleased to answer your questions and would be happy to provide any further assistance.

[The prepared statement of Mr. Rubinstein follows:]

Testimony of Ira Rubinstein

Adjunct Professor and
Senior Fellow, Information Law Institute
New York University School of Law

Legislative Hearing Examining H.R. 5777, the BEST PRACTICES Act, and the Boucher-Stearns Discussion Draft

Before the
Subcommittee on Commerce, Trade, and Consumer Protection

U. S. House of Representatives
July 22, 2010
2322 Rayburn House Office Building

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on H.R. 5777, the BEST PRACTICES Act, and the Boucher-Stearns discussion draft. My name is Ira Rubinstein and I am Adjunct Professor at New York University School of Law and a Senior Fellow at the Information Law Institute. I am grateful for the opportunity to appear before the Committee this afternoon and also for your efforts in developing comprehensive legislation that responds to growing public concern over privacy in the digital era.

I will focus my comments specifically on a key question in Congress' longstanding effort to regulate online privacy—what is the relationship between privacy legislation and industry self-regulation? To what extent should Congress encourage self-regulation by allowing alternative forms of compliance based on "safe harbor" provisions? Have existing safe harbor programs achieved their goals and, if not, how might they be changed to make them more effective?

Background: What is a Safe Harbor?

To answer these questions, I first need to say a few words about how safe harbors work, in theory and in practice. A safe harbor is a regulatory strategy under which a federal statute recognizes differences in industry performance explicitly by treating regulated firms who qualify more favorably than non-qualifying firms. In other words, safe harbors shield or reward firms if they engage in desirable behavior as defined by statute. Favorable treatment for better performing firms might include immunity from liability, protection from certain penalties,

exemptions from certain requirements, and/or permission to engage in certain desired behaviors. The key point to emphasize is that eligibility for the benefits conferred by a safe harbor are contingent upon a participating firm meeting a higher standard of performance than what is otherwise required of firms covered by the relevant statute.

In the privacy arena, the most familiar example of a safe harbor is the Children's Online Privacy Protection Act (COPPA). Section 5503 of this Act establishes an alternative means of compliance for operators that follow self-regulatory guidelines issued by an industry representative and approved by the Federal Trade Commission (FTC), subject to a notice and comment procedure. The COPPA safe harbor seeks to facilitate industry self-regulation in two ways: first, by granting enforcement-related benefits (operators that comply with approved self-regulatory guidelines are deemed to be in compliance with the law); and, second, by allowing greater flexibility in the development of self-regulatory guidelines in a manner that takes into account industry-specific concerns and technological developments. FTC approval of a COPPA safe harbor program turns on whether self-regulatory guidelines (1) meet or exceed statutory requirements; (2) include an effective, mandatory mechanism for the independent assessment of compliance with the guidelines (such as random or periodic review of privacy practices conducted by a seal program or third-party); and (3) contain effective incentives to ensure compliance with the guidelines (such as mandatory public reporting of disciplinary actions, consumer redress, voluntary payments to the government, or referral of violators to the FTC).

In practice, the COPPA safe harbor programs have met with success mainly in terms of complementing FTC's own enforcement efforts.[1] But the COPPA safe harbor also suffers from two serious shortcomings: First, a very low rate of participation (presumably because deemed compliance is not a strong enough incentive to persuade many firms to bear the costs of joining a safe harbor program and abiding by its guidelines when they have to comply with all but identical statutory requirements in any case);[2] and, second, a lack of regulatory flexibility (all of the approved self-regulatory programs have nearly identical requirements to those of the COPPA statute).

---

[1] *See* FTC, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS (2007) 24; *see also* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (forthcoming Winter 2011), 22-23 *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275 (describing the success of the CARU safe harbor program, which over an eight year period investigated and successfully resolved almost 200 cases).

[2] *See* Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 20-23 (noting that fewer than 100 firms have been certified under approved COPPA safe harbor programs).

One way to build on the success of the COPPA safe harbor programs while overcoming these two shortcoming would to adopt a more "co-regulatory" approach to privacy legislation, one in which industry enjoys greater scope in shaping self-regulatory guidelines, while government sets default requirements and retains general oversight authority to approve and enforce such guidelines. This approach envisions a more collaborative, flexible and performance-based model of self-regulation and explicitly draws on critical insights from environmental regulation.[3]

As noted above, COPPA safe harbor participants are subject to self-regulatory guidelines that are nearly identical to statutory requirements. Their incentives for joining are limited to deemed compliance and a largely empty promise of regulatory flexibility. In other words, COPPA failed in its efforts to treat safe harbor participants more favorably than other covered entities. In contrast, a co-regulatory approach would more effectively use both sticks and carrots as incentives. In the environmental setting, for example, sticks typically include a threat of stricter regulations or imposition of higher pollution fees, whereas carrots might take the form of more flexible regulations, recognition of better performance by the government, and cost-savings such as exemptions from mandatory reporting or easier and quicker permitting.[4] Firms that demonstrate high performance avoid these sticks and/or enjoy these carrots. How would this approach translate into the privacy arena and why it might attract industry support at much higher rates than that of the COPPA safe harbor programs?

A New Approach to Privacy Safe Harbors

Over the years, many advocacy groups and privacy scholars have favored a private right of action and liquidated damages as enforcement mechanisms in any new privacy legislation. Not surprisingly, industry has argued that such remedies are both unnecessary and ineffective. This suggests that an excellent stick might be devised around a tiered liability system. Under this new approach, privacy legislation would allow civil actions and liquidated damages awards against firms that engaged in prohibited practices and did not participate in an approved safe harbor program. In sharp contrast, compliance with approved self-regulatory guidelines would not only serve as a safe harbor in any enforcement action but exempt program participants from civil law suits and monetary penalties. Other sticks for non-participating firms might include broader opt-in requirements; external and independent audits of regulatory compliance and mandatory reporting to the FTC; and much stricter requirements for firms engaged in online behavioral advertising such as a total ban on the use of sensitive information in behavioral targeting and a data retention limit of one month.

[3] *Id.* at 28-36.
[4] *Id.* at 23

In addition to these sticks, privacy legislation might also offer safe harbor participants a number of carrots including exemptions from civil actions and liquidated damages; cost-savings such as compliance reviews based on self-assessments rather than external audits by an independent third-party; government recognition of better performing firms (e.g., an FTC "seal of approval" under which firms that meet safe harbor requirements are duly recognized); government procurement preferences for the products or services of participating firms (including perhaps contracts for cloud computing services); and regulatory flexibility in the form of tailored requirements addressed to specific business models such as online behavioral advertising (e.g., relaxed notice and consent and/or data retention requirements for firms that engage in practices similar to those described in Section 3(e) of the Boucher bill).

In summarizing this new approach to privacy safe harbors, it bears repeating that safe harbor benefits would be limited to firms demonstrating superior performance and would not be available to other covered entities that merely satisfy default statutory requirements. In other words, a safe harbor provides incentives, in the form of sticks and carrots, but only to firms that meet higher performance standards based on data governance principles, advanced privacy methodologies, and best practices. What might such standards look like?

Data governance may be defined as "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."[5] A good example of a data governance practice is appointing an individual (such as a Chief Privacy Officer) with overall responsibility for setting privacy protection policy and standards within a firm, managing risks and impacts of privacy-affecting decisions, publicizing within the company who has authority and accountability for governance decisions, and creating reporting mechanisms for both internal and external stakeholders about the status within the organization of such policy and standards.

Advance privacy methodologies include development guidelines for building privacy protection into any product or service that uses personal data. This process—which is sometimes referred to as "Privacy by Design"—implies that before releasing a new product or service, firms identify and address privacy issues using well-established techniques including data minimization, anonymization, access controls, and encryption and other security measures; create a privacy statement describing how personal data will be handled in response

[5] *See* Data Governance Inst., Defining Data Governance, *available at* http://www.datagovernance.com/gbg_defining_governance.html.

to identified privacy concerns; and otherwise protect consumers' privacy by applying all relevant aspects of a robust set of Fair Information Practices (FIPs).[6]

Finally, industry-wide best practices include mandatory privacy training for all staff with privacy responsibilities, providing online guidance on privacy and security issues to employees and consumers, and implementing a complaint-handling procedure. Both of the bills under consideration today require safe harbor participants to adopt best practices. (In Section 3(e) of the Boucher-Stearns draft bill, however, the safe harbor provision is limited to online advertising firms; hence the focus instead is on *industry-specific* best practices.)

It is important to note that this is a very partial list of relevant performance standards. A more comprehensive list of potential standards is available in the previously mentioned article.[7]

Public Consultation Requirement

In thinking about this new approach to privacy safe harbors, two additional caveats are necessary: First, unlike previous or existing self-regulatory schemes, it would not suffice for industry alone to develop the relevant privacy performance standards or best practices. Rather, such standards must emerge from a multi-stakeholder process in which both advocacy groups and members of the public have an opportunity to participate. This requires that interested parties engage in difficult and perhaps protracted negotiations, and stay at the table until a consensus is forged.[8] Second, the government must reserve the final decision on whether the performance standards or best practices achieve a high enough level of privacy protection to warrant the granting of any proposed safe harbor benefits.

The COPPA safe harbor relies on a notice and comment procedure to approve proposed self-regulatory guidelines, but it is worth considering two alternative options that meet both of the above caveats. The first is negotiated rulemaking, a statutorily defined process by which agencies formally negotiate rules with regulated industry and other stakeholders as an alternative to conventional, notice and comment rulemaking.[9] In theory, negotiated rulemaking

---

[6] *See, e.g.,* U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (identifying eight principles: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability and auditing).

[7] *See* Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes,* 49-50.

[8] This may seem impracticable, but three leading Internet firms recently partnered with a diverse group of non-governmental actors in a voluntary effort to negotiate free speech and privacy principle. After eighteen months of work, this multi-stakeholder group reached agreement and launched the Global Network Initiative (GNI), jointly committing to a set of principles and implementation guidelines as well as an accountability system based on independent, third-party assessments. For the GNI's three core commitment documents, *see* http://www.globalnetworkinitiative.org/index.php.

[9] *See* the Negotiated Rulemaking Act of 1990, codified as amended at 5 U.S.C. §§ 561-570.

reduces cost and other regulatory burdens by developing alternative or innovative means of compliance not permitted under a statute's default requirements, thereby allowing industry more flexibility as to the timing of compliance investments, and reducing regulatory uncertainty. The incentives for regulators and advocacy groups to support this approach include the prospects of a higher level of benefits than would have been obtained, as a practical matter, under the standard default requirements.[10]

Negotiated rulemaking is most likely to succeed when two additional conditions are present: First, the regulatory agency should understand the industry and the issues well enough to have formulated a broad view of what a good regulatory solution should look like but it should not be wedded to a particular substantive outcome. Second, the substance of the regulation should require the credible transmission of information between the regulated entities and other interest groups--i.e., industry should possess unique knowledge and expertise such that it is in the best position to understand how regulation will affect its activities. Hence, industry cooperation is needed to ensure a satisfactory regulatory outcome.

Arguably, the present case satisfies both of these conditions. On the one hand, the FTC is very knowledgeable regarding online privacy but is not yet locked-in to any one approach. On the other, Internet firms (including network advertising firms) undoubtedly possesses greater expertise and insight into the complex technology and evolving business models underlying the digital world than either privacy advocates or FTC staff. In the past, this information has been shared or elicited mostly through one-sided communications—unilateral industry codes of conduct; complaints filed with the FTC; or charges and countercharges at public forums. In a (successful) negotiated rulemaking process, however, the parties have an incentive to educate each other, pool knowledge, and cooperate in problem solving.

That said, negotiated rulemaking is not always appropriate and imposes heavy burdens on participants in terms of time and other resources. With these burdens in mind—and especially their impact on the FTC's relatively small Division of Privacy and Identity Protection—I would like to propose an alternative to negotiated rulemaking that both addresses potential resource concerns while ensuring that the safe harbor approval process establishes a role for advocacy groups and the public.

In a nutshell, this second alternative consists in a two-step process for approving privacy safe harbors. In Step 1, safe harbor program sponsors would have to submit to the FTC a short initial proposal showing that they have met statutorily defined criteria (see below). FTC would

[10] *See* Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes,* pp. 44-46.

then have 45 days to conduct a fairly perfunctory review designed to determine if these criteria were met. If not, FTC would issue a preliminary denial and the sponsor would have to wait twelve months from the FTC decision before submitting a revised proposal; if so, FTC would issue a preliminary approval and the sponsor would then proceed to Step 2. The criteria for approving an initial proposal might include the following:

- The sponsor is representative of an industry sector. (This is intended to discourage applications from firms that wish to sponsor a safe harbor program merely as part of a business plan, rather than due to their industry role or subject matter expertise);
- The sponsor has industry support as indicated by endorsements from leading members of the industry (defined in terms of size, revenue, influence, etc.);
- The sponsor's proposed program advances broad goals such as consumer protection, cost savings, and innovation;
- The sponsor has drafted self-regulatory guidelines addressing all of the core statutory requirements of a safe harbor program.[11]

Upon approval of an initial proposal, the sponsor would then have up to 180 days to submit a more detailed application for approval, which FTC would review and approve within 180 days using a conventional rulemaking process. Step 2 would require the sponsor to submit a more comprehensive program description demonstrating that the program meets or exceeds all relevant safe harbor requirements. In addition, the sponsor would have to show that it continues to have substantial industry support (e.g., by listing the names of the firms that have expressed an interest, in writing, in participating in the program) and that it has engaged in stakeholder consultation. This would require the sponsor to include in its formal application a statement describing who is affected by the proposed safe harbor guidelines, efforts it has taken to consult with affected groups (including consumer or advocacy groups), changes to the proposed safe harbor guidelines resulting from these consultations (if any), a summary of any issues that remain unresolved and why (including any concerns raised by the FTC), and that the public consultation remained open for at least 60 days.[12]

---

[11] This assumes that FTC would engage in a rulemaking procedure defining industry representation, consumer benefits, cost savings, and innovation.

[12] The Network Advertising Initiative recently engaged in a public consultation along these lines when it released a draft update to its original NAI Principles, solicited public comments on the proposed changes, and published both the comments and its responses. *See* NAI, NAI PRINCIPLES 2008: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT FOR ONLINE BEHAVIORAL ADVERTISING (Apr. 2008), *available at* http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf. Under the process described in the text, however, FTC would retain final approval authority if it decided the NAI guidelines were inadequate notwithstanding a satisfactory public consultation.

Step 1 of this alternative process is meant to discourage the submission of weak applications by entities lacking industry expertise or support. It also dispenses with the need for FTC to work with sponsors on improving inadequately designed programs.[13] FTC would review the initial proposal mainly to ensure that it is approvable subject to meeting the more formal requirements of Step 2. But if the program is inadequate on its face, FTC would simply deny the initial application and impose the 12-month waiting period. Step 2 requires industry to reach a rough consensus with advocacy groups and respond to any major concerns or to explain why this is infeasible. Although FTC is not required to approve a program merely because industry demonstrates good faith efforts in the consultation process, the idea is that by requiring a rough consensus, the consultation process will result in better quality guidelines with greater legitimacy for everyone involved. The overall goal is to ensure that FTC devotes its limited resources to reviewing programs that have already demonstrated a high likelihood of success.

Comments on the Safe Harbor Provisions of the Two Bills Now Under Consideration

When Congress last seriously considered online privacy legislation about ten years ago, bills introduced by Reps. Markey, Sens. Burns and Widen, Rep. Stearns, and Sen. Hollings provided for a comprehensive, self-regulatory safe harbor modeled on COPPA.[14] Like these earlier bills, both of the bills under consideration today include safe harbors but of very different scope and import. Section 3(e) of the Boucher bill creates a limited safe harbor for advertising networks that track online behavior. It exempts these networks from having to obtain explicit, opt-in consent provided they allow consumers to access and manage their profiles.[15] A coalition of consumer groups has objected to this provision on the grounds that it relies on the discredited notice-and-choice model, which they consider ineffective for ensuring

[13] The privacy safe harbor might also include a provision encouraging or requiring FTC to convene a privacy workshop at least once every 5 years, where it would consider recent developments in privacy and technology and to issue a report on how best to improve privacy regulation. One goal of these workshops (which would resemble the most recent FTC Privacy Roundtables) would be to identify industry sectors that are "ready" for safe harbor programs, thereby encouraging such groups to submit initial proposals.

[14] *See* the Electronic Privacy Bill of Rights Act of 1999, H.R.3321, 106th Cong. § 4 (1999); the Online Privacy Protection Act of 1999, S. 809, 106th Cong. § 3 (1999); Consumer Privacy Protection Act of 2002, H.R. 4678, 107th Cong. §106 (2002); the Online Personal Privacy Act, S. 2201, 107th Cong. § 203 (2002).

[15] More specifically, the requirements for "individual managed preference profiles" under Section 3(e) are as follows: (1) users must be provided with a readily accessible opt-out mechanism whereby the opt-out choice of the individual is preserved and protected from incidental or accidental deletion; (2) firm must delete or render anonymous any covered information not later than 18 months after the date the covered information is first collected; (3) firms must place a symbol or seal in a prominent location on both its website and on or near any ads it delivers based on a user's preference profile that enables an individual to connect to additional information regarding advertising practices and allows individuals to review and modify, or completely opt out of having, a preference profile created and maintained by the firm or a an ad network; and (4) any ad network to which a firm discloses covered information must avoid further disclosure to any other entity except with the user's express affirmative consent.

online privacy.[16] In my view, the more fundamental problem with this approach is its narrowness and inflexibility. Section 3(e) enshrines a single program already adopted by several companies engaged in targeted advertising (including Google and Yahoo, both of whom already allow users to access and revise their profiles). But the Boucher bill lacks a more general safe harbor provision that would encourage other companies (and other sectors) to offer innovative privacy protections or adopt industry-specific best practices.

In contrast, Title V of the Rush bill provides a full-fledged safe harbor under which any self-regulatory program (referred to as a "Choice Program") may qualify for certain exemptions provided the programs meet the following five requirements:

- A "universal" opt-out mechanism and preference management tool that applies an individual's choices to all firms participating in the Choice Program;
- Guidelines and procedures that offer equivalent or greater protections than those required in Title I (transparency, notice and individual choice) and Title II (accuracy, access and dispute resolution);
- Approval procedures for participating firms;
- Procedures for periodic self-assessment and random compliance testing; and
- Consequences for failure to comply with program requirements.

Firms that participate in and comply with an approved Choice Program meeting these requirements are exempted from (1) the express affirmative consent requirements under subsection 104(a); (2) the access requirement under section 202(b); and (3) liability in a private right of action brought under section 604.

In my opinion, the Choice Program is preferable to the limited exemption for individual managed preference profiles for several reasons. First, and obviously, it is more comprehensive and therefore allows companies in any sector to develop innovative privacy protections or adopt industry-specific best practices. Second, it relies on a good mix of carrots and sticks including tiered liability. However, in order to meet the basic test of any safe harbor--which is that program participants are entitled to better treatment based on superior performance--the Choice Program needs strengthening in several areas. To begin with, it needs to clarify that safe harbor approval depends on compliance not only with Titles I and II but also with Title III (security, data minimization and accountability). I would also support the addition of several new elements to the list of requirements for self-regulatory programs including (a) procedures for handling and reporting on consumer complaints; and (b) guidelines for requiring

[16] *See* Letter from Jeff Chester, Center for Digital Democracy, et al., to Reps. Rick Boucher and Cliff Stearns (June 4, 2010), *available at* http://www.democraticmedia.org/files/u1/2010-06-letter-to-boucher.pdf.

participating firms to build privacy protection into their products or services using "privacy by design" or related methods and techniques.

Recommendations and Conclusion

First, Congress needs to enact comprehensive privacy legislation incorporating the full range of Fair Information Practices.

Second, this legislation should include a broad-based safe harbor program based on a co-regulatory approach that provides flexibility to industry in shaping self-regulatory guidelines in exchange for superior performance, while ensuring that the FTC retains general oversight authority to approve and enforce such guidelines.

Finally, this safe harbor program should be amended to include a complaint handling process and privacy by design requirement; it should also require public consultation as part of the safe harbor approval process, which might consist in negotiated rulemaking or the two-step application process as described above.

Section 3(e) of the Boucher-Stearns discussion draft and the Choice Program as set out in Title IV of H. R. 5777 are important first steps in developing a new approach to safe harbors but should be expanded in various ways as discussed above.

I want to thank you again for the opportunity to appear before the Committee today. I will be pleased to answer your questions and would be happy to provide any further assistance as appropriate.

Mr. RUSH. Mr. Zaneis, you are recognized for 5 minutes.
Mr. ZANEIS. I am happy——
Mr. RUSH. I am sorry——
Mr. ZANEIS. That is all right, we don't want to skip over Jason.
Mr. RUSH. Mr. Goldman, I am sorry. Mr. Goldman——
Mr. GOLDMAN. Thank you very much.
Mr. RUSH. You are recognized for 5 minutes.

STATEMENT OF JASON GOLDMAN

Mr. GOLDMAN. Good afternoon, Chairman Rush, Ranking Member Whitfield, and members of the Subcommittee. I am Jason Goldman, Telecommunications, and E-commerce Counsel at the U.S. Chamber of Commerce. The U.S. Chamber of Commerce is the world's largest business federation representing the interest of more than three million businesses and organizations of every size, sector, and region. On behalf of the Chamber and its members, I thank the Subcommittee for its work on consumer protection and for the opportunity to testify here today.

Privacy is a key issue for the Chamber. The Chamber supports policies that foster business opportunities while respecting consumer's privacy. The collection of personal information is necessary to provide consumer, social, and business benefits. Given the diversity of private sector businesses should have latitude within acceptable guidelines in defining what they need—what kind of information they need to collect and use.

Recently the debate over privacy has been brought to the forefront by the growth of the Internet. The Internet has revolutionized the way business is conducted in all sectors of the global economy including financial services, retail, wholesale distribution, and manufacturing. Today the vast majority of companies, small and large, are online and use the Internet to communicate with consumers and with the vendors, and all the different other entities. In particular, ad-supported content has been key to the success of broadband. Frequently online content is provided free of charge to consumers and revenues are instead generated through advertising. This ad-supported business model has been a key to the success of many Internet adventures and has helped to make the Internet an engine of growth in the U.S. economy.

I will now turn to the bills that are the topic of this hearing. The Chamber received the text of the Best Practices Act just a few days ago, so my comments today are based on our initial read of the bill and may change as we further analyze the bill and vet the bill through our membership. The Chamber's analysis of Boucher/Stearns discussion draft was submitted to their Subcommittee in June and is attached to our testimony.

The Chamber very much appreciates the work that went into drafting the Best Practices Act. Despite the inclusion of some of the provisions that we support, we still have strong concerns the bill as currently drafted. The Chamber—I will go through some of the provisions that we support and also some of the ones that we have modifications to. The Chamber is pleased that the bill directs the FTC to promulgate rules under this act in a technology-neutral manner. Government should not pick winners and losers. The Chamber applauds the inclusion of language that preempts State

laws governing the collection and use of data. However, the Chamber believes the language could have been even stronger to help businesses avoid having to comply with 50 different State laws. The Chamber agrees with the intent of Section 502 which states that the bill should have no effect on activities covered by other federal privacy laws. However, the opening clause of this section states "except as provided expressly in the Act." This could be interpreted by the FTC or by the courts as permitting the creation of multiple layers of regulation.

The Chamber appreciates the bill attempts to maximize regulatory flexibility. However, at the same time the Chamber is concerned that the sheer number of rulemakings will create needless regulatory uncertainty. The Chamber also believes that the safe harbor provision as drafted is a good start but improvements could be made. We are gratified by the recognition that industry self-regulation in this area has and will continue to protect consumers, however the safe harbor in our opinion is too narrow and should follow FTC and industry principles. And also the Chamber has serious concerns about private right of action as well as an explicit grant of authority to State Attorneys General to enforce the legislation.

When combined with the FTC's own enforcement authority we are concerned that these official mechanisms will serve to impose duplicative and potentially inconsistent findings of liability as well as excessive damage awards. In addition the explicit grant of authority for the award of punitive damages and attorney's fees will serve to increase the likelihood that elements of the plaintiff's class action trial bar will use this legislation as a way to increase class action litigation with little benefit being given to the general public.

The Chamber also has some concerns covered in more detail in our testimony with the opt-in requirements of third party sharing and opt-out requirements for information collection, as these provisions could upset established business practices for many of our members.

Finally the Chamber has concerns with access and dispute resolution and the definition of covered information which I will be happy to discuss further during our Q and A. Thank you again, and I am happy to answer your questions following Mr. Zaneis.

[The prepared statement of Mr. Goldman follows:]

Statement of the U.S. Chamber of Commerce

ON: H.R. 5777, THE "BEST PRACTICES ACT" AND H.R. ___, A DISCUSSION DRAFT TO REQUIRE NOTICE TO AND CONSENT OF AN INDIVIDUAL PRIOR TO THE COLLECTION AND DISCLOSURE OF CERTAIN PERSONAL INFORMATION RELATING TO THAT INDIVIDUAL

TO: UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BY: JASON D. GOLDMAN
COUNSEL, TELECOMMUNICATIONS & E-COMMERCE
U.S. CHAMBER OF COMMERCE

DATE: JULY 22, 2010

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business – manufacturing, retailing, services, construction, wholesaling, and finance – is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 113 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

Hearing on H.R. 5777, the "BEST PRACTICES Act" and H.R. ___, A Discussion Draft to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to that Individual

Testimony of Jason D. Goldman
Counsel, Telecommunications & E-Commerce
U.S. Chamber of Commerce

July 22, 2010

Good afternoon, Chairman Rush, Ranking Member Whitfield, and other Members of the Subcommittee on Commerce, Trade, and Consumer Protection. I am Jason D. Goldman, Telecommunications & E-Commerce Counsel at the U.S. Chamber of Commerce, the world's largest business federation, representing the interests of more than three million businesses and organizations of every size, sector, and region. On behalf of the Chamber and its members, I thank you for the opportunity to testify here today on the "BEST PRACTICES Act" and on a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

Chamber's Position on Privacy

The Chamber supports policies that foster business opportunities while respecting consumers' privacy. The collection of personal information is necessary to provide consumer, social, and business benefits. Given the diversity of the private sector, business decision makers should have latitude, within acceptable guidelines, in defining their needs for personal information. Cost control and competitive pressure in the private sector provide a strong natural deterrent to the collection of unnecessary, erroneous, or irrelevant information.

Public policymakers and business leaders should weigh protection of privacy rights against a variety of factors, such as consumer convenience, the needs of management and the ultimate cost to the individual and public at large as well as to business and governmental entities. Before proposing governmental actions, policymakers should have a thorough understanding of the possible tradeoffs of these factors.

The Importance of the Internet to the U.S. Economy

The Internet has revolutionized the way business is conducted in all sectors of the global economy—including financial services, retail, wholesale-distribution, manufacturing, and many more. Today, the vast majority of companies of all shapes and sizes are online in some capacity and use the Internet to communicate with consumers, employees, existing customers, potential customers, and business partners around the world.

In particular, ad-supported content has been key to the success of broadband. With broadband accessible to the vast majority of Americans, the amazing array of content (including applications and services) available on the Internet has convinced more and more Americans to

go online using a broadband connection every year. Frequently, online content is provided free of charge to consumers, and revenues are instead generated through advertising. U.S. Internet advertising revenues totaled $5.9 billion for the first quarter of 2010, representing a 7.5 percent increase over the same period in 2009, according to the Interactive Advertising Bureau and PricewaterhouseCoopers. Some of the products that consumers receive for free are: Web mail, maps, news sites, blogs, social networks, video, job boards, and product rating and pricing services. Consumers recognize and appear willing, in many situations but not all, to permit information to be collected about them in exchange for goods and services that are of value to them. This ad-supported business model has been a key to the success of many Internet ventures and has helped to make the Internet an engine of growth in the U.S. economy.

Analysis

The Chamber received the text of the BEST PRACTICES Act earlier this week, so the comments below are based on our initial read of the bill and may change as we further analyze the language and vet the bill through our membership. The Chamber's analysis of the Boucher/Stearns discussion draft was submitted on June 2, 2010, to the House Subcommittee on Communications, Technology and the Internet, and is attached to this testimony (Appendix A).

BEST PRACTICES Act

The Chamber appreciates the work that went into drafting the BEST PRACTICES Act. Despite the inclusion of some provisions that we support, we have strong concerns with H.R. 5777 as currently written.

I. Definition of Covered Information

The definition of "covered information" in H.R. 5777 should be narrowed. Only data elements that could be used to commit identity theft or other direct consumer harm should be included in the definition. If the "unique identifier" is publicly available and does not contain any personal information then it should be excluded from the definition. For example, as drafted, the bill would impose the same protections on user IDs as it would for name and email addresses.

Therefore, "unique identifier," "persistent identifier," "Internet Protocol address," "telephone number," "fax number," and other such data elements should be removed from the definition except where such data has already been merged with other personal information elements.

The Chamber supports standardized definitions. Therefore, rather than creating a new category of "covered information," it would be better to model this definition after the "personal information" definitions found in many recent state data security and breach notification bills. Instead of including general categories of data elements which cannot identify a person, these definitions tend to tie a person's first and last name or first initial and last name with an address to a data element such as a social security number, drivers' license number, or financial account number.

The Chamber supports the exemption from the "covered information" definition for information collected about an employee, by an employer, prospective employer, or former employer that directly relates to that relationship.

II. Definition of Operational Purpose

Generally, the "operational purpose" exemption is too limited because it does not apply if the data is also used for marketing, advertising, or sales; dual-use of such data is a common industry practice. Under the bill, if a user chooses to opt-out, then the collection of non-identifying information (e.g., cookies or the user's IP address) is prohibited.

III. Definition of Sensitive Information

Instead of codifying precise geographical information as sensitive personal information, the Chamber recommends that the collection and use of this data be governed by self-regulatory regimes.

IV. First-Party Opt-Out Requirement

Consumer privacy expectations are different when dealing directly with a first-party then when there is a third-party relationship between the consumer and the business. For this reason, the U.S. regulatory framework has long recognized a broad first-party exemption to consumer consent requirements which has been supported by the Federal Trade Commission (FTC) as recently as in its staff report on online behavioral (OBA) advertising principles. The Chamber believes this legislation should maintain this first-party exemption.

U.S. businesses would be adversely impacted by a first-party opt-out mandate. It would require all media, retailers, service-oriented businesses, marketing companies, advertisers and others—in both online and offline environments—to offer an opt-out option to all consumers for any data that may be collected or used under any circumstances. Furthermore, H.R. 5777 should allow for flexibility to account for the inherent differences between operating in the offline and online worlds.

Also, opting out of the collection of certain information could impact Web site operation and optimization. For example, when a consumer voluntarily visits a Web site, certain information must be collected by that company, including their IP address or referrer URL, in order to deliver the content on the site.

An opt-out consent standard would create a perverse incentive of requiring all media, retailers, service-oriented businesses, advertisers and others—in both online and offline environments—that do not already collect detailed consumer information to begin doing so in order to allow them to exercise opt-out choices over time. Such a requirement, for instance, could require retailers to offer all credit-card-using consumers opt-outs for the use of bar code scanners at checkout counters. In turn, these businesses would begin to develop and maintain detailed dossiers of personal transactions, in order to render all data from past transactions

unusable if at any point in the future the consumer wishes to exercise an opt-out with respect to the prior collection of data.

The Chamber does not believe that such a statute would further consumer trust; rather it may create greater privacy concerns while costing businesses millions of dollars to implement.

V. Express Affirmative Consent

Requiring opt-in "express affirmative consent" for the disclosure of "covered information" to unaffiliated third parties profoundly alters commonly accepted business practices. The definition of covered information is extremely broad as stated previously and includes several largely anonymous types of data, including cookies, IP addresses, and unique identifiers for computers or devices. These types of data points are inherently neither personal nor sensitive in nature and, thus, should not be subject to the strictest consumer consent requirements. Current regulatory requirements subject only the most sensitive data categories to an opt-in requirement, and many of those provisions recognize a lower standard when that data is used for marketing or advertising purposes.

VI. Access and Dispute Resolution

To avoid redundancy and confusion, there should be an exemption from the access and dispute resolution requirements when an entity or information (e.g., databases containing public record data) is already regulated by other laws (mainly consumer reporting agencies under Fair Credit Reporting Act and financial institutions under Gramm-Leach-Bliley). Additionally, databases that are used for fraud, authentication, and contract enforcement should be exempted, to the extent necessary, to prevent fraudsters from accessing and/or modifying these databases. Once all of these exemptions are included, however, mainly just advertising databases would be subject to this new access and correction regime. Therefore, we would encourage policymakers to carefully study this issue before proceeding because the cost of providing access and correction for those databases is very steep, while the benefit for consumers is minimal.

VII. Safe Harbor

The Chamber believes that the safe harbor provision, as drafted, is a good start but improvements could be made. We are gratified by the recognition that industry self regulation in this area has and can continue to protect consumers. However, the safe harbor is too narrow and should follow FTC and industry principles, including the exemption of first party data practices, greater flexibility in how consumer notice is delivered, and exemption from data accuracy and correction provisions (it appears to only exempt companies from the data access requirements). Moreover, the recognition that an opt-out standard for third-party data usage sufficiently protects consumers' privacy calls into question whether the opt-in standard for third-parties in Section 104 is proper. The FTC and industry agree that opt-out is the appropriate standard, so we would urge the Chairman to seek to codify that standard as the baseline in H.R. 5777.

VIII. Activities Covered by Other Federal Privacy Laws

The Chamber agrees with the intent of Section 502, which states that H.R. 5777 should have no effect on activities covered by other enumerated federal privacy laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and HIPAA. However, the opening clause of this section, which states "except as provided expressly in this Act," could be interpreted by the FTC or by courts to permit the creation of another layer of regulation in addition to provisions in each of the enumerated acts. Given the potential conflicts with having the same type of data collection and use covered by more than one federal privacy regime, a covered entity could very well find itself unable to comply with two separate federal privacy laws for the same covered information, thereby involuntarily subjecting itself to fines and other enforcement actions for non-compliance with one or both of the acts. To avoid this potential conflict with existing federal privacy regimes, the Chamber strongly recommends that this section be clarified to provide an explicit carve-out from the definition of covered entity for entities already covered by the enumerated acts.

IX. Private Right of Action

The Chamber also has serious concerns about the various liability-related provisions in H.R. 5777. For example, in addition to the robust enforcement mechanisms provided to the FTC, the legislation also contains a private right of action as well as an explicit grant of authority to state attorneys general to enforce the legislation. We are concerned that all of these mechanisms will serve to impose duplicative and potentially inconsistent findings of liability as well as excessive damage awards. In addition, the explicit grant of authority for the award of punitive damages and attorney's fees will serve to increase the likelihood that elements of the plaintiffs' class action trial bar will use this legislation as a way to increase class action litigation with little benefit being given to the general public.

X. FTC Rulemaking Authority

The Chamber is pleased that H.R. 5777 directs the FTC to promulgate rules under this Act in a technology-neutral manner. Specifically, the bill prohibits the FTC from requiring the deployment or use of any specific products or technologies, including any specific computer software or hardware.

The Chamber appreciates that the bill attempts to maximize regulatory flexibility by granting the FTC authority to engage in rulemakings on a variety of matters. Given that business must respond rapidly to market developments and technological advancements, innovation should be encouraged, not hindered. However, at the same time, the Chamber is concerned that the sheer number of rulemakings will create needless regulatory uncertainty. In addition to rulemakings to create exemptions and exceptions, there are rulemaking requirements in many other areas of the bill including definitions (e.g., sensitive information and third parties), on notice, on accuracy, and on the process for granting safe harbor for self-self-regulatory initiatives.

XI. Effect on Other Laws

The Chamber applauds the inclusion of language that would preempt state laws governing the collection and use of data. However, the Chamber believes this language could be even stronger to help businesses avoid the complexity of having to comply with 50 different laws.

Conclusion

Once again, the Chamber greatly appreciates the opportunity to testify today. The Chamber stands ready to work with you on these and other issues. Thank you very much.

Appendix A

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

June 2, 2010

The Honorable Rick Boucher
Chairman
Subcommittee on Communications,
Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications,
Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Boucher and Ranking Member Stearns:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, thanks you for the opportunity to offer thoughts and recommendations on your draft privacy legislation.[1] The draft legislation would fundamentally change how online and offline information collection and sharing is conducted, and has the potential to harm a vibrant and legitimate part of the U.S. economy. In addition, close scrutiny is needed to determine the bill's impact on existing laws. While the Chamber is pleased that the draft bill contains appropriate provisions to ensure predictable and consistent enforcement, the Chamber has some strong concerns with the draft bill that are highlighted below.

Definition of Covered Information

The Chamber believes that, as currently drafted, the definition of "covered information" is far too broad. It is important that such a definition encompass only data elements that could be used to commit identity theft or other direct consumer harm. Furthermore, the draft bill includes the term "unique identifier" within the definition of covered information. Such a term is overly broad as many social media websites assign each user a unique identifier that is publicly available and absent of any personal information. The bill would impose the same protections on user IDs as it would for name and email addresses.

Therefore, the Chamber strongly urges that data elements such as "unique identifier," "persistent identifier," "Internet Protocol address," "telephone number," and "fax number" be

[1] The Chamber represents many different types of companies and economic sectors with different concerns in the telecommunications and Internet areas and while the position stated in these comments is the official position for the U.S. Chamber of Commerce, our comments do not reflect the views of all company members.

removed from the definition except where such data has already been merged with other personal information elements. As an example, a persistent identifier on a device owned by an individual could literally cover a product code. Additionally, "covered information" appears to be a new definition that is not used by any other relevant privacy law. The Chamber is concerned about the conflicts and confusion that could arise from the use of this broad, new definition covering nearly all data.

A more appropriate way to approach the scope of covered information would be to craft a definition similar to "personal information" definitions found in many recent state data security and breach notification bills. These definitions tend to tie a person's first and last name or initial and last name with an address to a data element such as a social security number, drivers' license number, or financial account number. Within this type of definition there are data elements that can actually identify a specific person, as opposed to general categories of data elements which cannot identify a person.

Additionally, the definition of "personally identifiable information" should specifically exclude any personal information that has been rendered anonymous or "de-identified" prior to its use. This type of information is excluded from other federal privacy laws, such as the Health Information Portability and Accountability Act (HIPAA). Under HIPAA's de-identification standard, personal health information that has been de-identified in compliance with the law's prescribed standards is not subject to the HIPAA privacy rules. The Chamber recommends a similar de-identification standard be used in this legislation and believes this is the correct standard for public policy reasons, as well as to avoid direct conflicts on this issue in federal law, as discussed further below.

First Party Opt-Out Requirement

The Chamber is concerned that the proposal requires a "covered entity"—defined to include nearly every commercial business of even moderate size (i.e., those with more than 5,000 customers annually)—to obtain consumer consent prior to the collection and use of any customer information. The federal government has long recognized that consumers have a direct relationship with first parties that they chose to do business with and that their privacy expectations are different than when third parties are involved. For example, when a consumer voluntarily visits a Web site, certain information must be collected by that company, including their IP address or referrer URL, in order to deliver the content on the site. This information will be used by the first party Web site for non-transactional purposes, including Web site optimization and internal marketing practices. For this reason, the U.S. regulatory framework has long recognized a broad first-party exemption to consumer consent requirements which has been supported by the Federal Trade Commission (FTC) as recently as in its staff report on online behavioral (OBA) advertising principles. The Chamber believes this first-party exemption should be maintained in the current legislative proposal.

The impact to U.S. businesses from a new, statutorily-mandated consent standard for first parties would be vast. It would require all media, retailers, service-oriented businesses, marketing companies, advertisers and others—in both online and offline environments—to offer a detailed menu of opt-out options to all consumers for any data that may be collected or used

under any circumstances. Opting out of these uses of covered information would have several unintended consequences, including hindering fraud prevention, disabling basic Web site monitoring and advertising metrics, and hampering content customization and retail product recommendations online.

For example, such a requirement could require retailers to offer all credit-card-using consumers opt-outs for the use of bar code scanners at checkout counters. A bottom-line concern is that it is unclear which activities trigger a choice requirement. Many direct marketing activities already require choice under various federal laws or industry practices. In the draft bill, choice is required for marketing, advertising, and sales purposes. However, choice is not required for data analytics for product improvement—which is typically performed to improve sales.

Lastly, an opt-out consent standard would create a perverse incentive of requiring all media, retailers, service-oriented businesses, advertisers and others—in both online and offline environments—that do not already collect detailed consumer information to begin doing so in order to allow them to exercise opt-out choices over time. This, in turn, would require these businesses to develop and maintain detailed dossiers of personal transactions, in order to render all data from past transactions unusable if at any point in the future the consumer wishes to exercise an opt-out with respect to the prior collection of data. The Chamber does not believe that such a statute would further consumer trust; rather it may create greater privacy concerns while costing businesses millions of dollars to implement.

Notice and Consent for Offline Information

The Chamber strongly agrees that privacy principles should be applied to the collection and use of information in both the online and offline environments. However, any such legislative or self-regulatory regimes must be flexible enough to recognize the inherent differences that technology plays in each environment. Whereas the online environment is interactive and allows a link to a Web page that can deliver a privacy policy and offer choices for information use, the offline environment is much different, particularly when businesses employ manual or small-scale data collection devices, such as "3x5" survey or warranty cards inserted into magazines and publications. A privacy policy or notice in the form proposed by the legislation cannot reasonably be delivered on such collection devices, and choice cannot be obtained unless the consumer has access to the terms and conditions of the privacy notice. Another example involves the use of security cameras in stores that also monitor wait-time-in line at checkout to speed sales transactions for customers. It would not be feasible to provide a lengthy notice of privacy practices or choice prior to data collection. Simply put, in the offline arena, covered information may be collected in different formats and technologies, so more flexibility is needed for the timing and content of notice and how and where to offer choice.

In addition to the type of notice and consent to be provided in the online and offline settings, the proposed legislation must also consider the ability for businesses to comply with a notice prior to collection of covered data. For example, in both the online and offline environments, it is often impossible to deliver a notice before information collection begins. The above examples demonstrate this impracticality for the offline world but, importantly, this

impracticability is true in the online environment, too. Data collection begins immediately when a consumer enters a Web site address in a browser and clicks the go or return function, as an IP address must be collected before a Web site can be delivered to the browser for display. Also, each third party conducting business on the Web site, whether for marketing, fraud detection, or setting a time and data stamp, begins collecting information before the Web site actually loads. Therefore, significant amounts of covered information, as defined in the proposed bill, could be collected before a consumer would actually read a privacy policy and be able to make a choice. In many cases, consumers rarely if ever choose to read a privacy policy, so presumably all data collected to display the Web site would be in violation of the proposed law.

These practical problems need to be addressed before legislation is introduced, and the Chamber recommends eliminating any requirement that notice be provided prior to the "collection" of data. Many federal privacy laws, for example, set forth notice requirements in connection with businesses' uses of information for particular purposes in order to avoid such impracticalities of placing notice and consent regimes on the broad collection of data prior to its use. The Chamber recommends a similar focus on the use of data as further discussed below.

Concerns with Collection Restrictions

The language in Section 3 is focused on both the collection and use of covered information. There are major technological hurdles that companies in the online space would face to comply with the limitations on collection of covered information.

When a user decides to go to a Web page from a Web site, routine information is usually collected to help deliver and display that Web page. The collection of this data is integral to the proper and efficient delivery of Web pages; therefore, there could be tremendous technical ramifications if a consumer blocks the transmission of this data when selecting an opt-out option.

Advertising revenue frequently allows Web sites to offer consumers content for free. This ad-supported business model has been a key to the success of many Internet ventures and has helped to make the Internet an engine of growth in the U.S. economy. Unfortunately, the draft bill would disrupt this pro-consumer business.

Generally, the "operational purpose" exemption in the draft is too limited because it does not apply if the data is also used for marketing, advertising, or sales; dual-use of such data is a common industry practice. Under the draft, if a user chooses to opt-out, then the collection of non-identifying information (e.g., cookies or the user's IP address) is prohibited. However, in the offline world, non-identifiable user information is not subject to notice and choice used to target advertising displayed in magazines, newspapers, and billboards. The draft bill should be technology-neutral and should not favor one type of advertising over another.

Express Affirmative Consent for Disclosure of Covered Information

Numerous laws, including the Cable Communications Policy Act, Telecommunications Act, Gramm-Leach-Bliley Act, and Fair Credit Reporting Act allow business to share customer or other information with unaffiliated businesses whether for a "permissible purpose" or

otherwise. This draft would cover broadly all disclosures of customer or other covered information without regard for any intended purpose or to protect any perceived harm. It is unclear how the preemption language in this law could be followed with respect to these other legal information sharing allowances. By restricting this existing information flow, numerous businesses would be affected, especially small and local businesses that regularly use marketing lists for market research or direct mail prospecting.

No Opt-In for Sharing with Unaffiliated Third Parties

As currently drafted, the proposal requires opt-in "express affirmative consent" for the disclosure of "covered information" to unaffiliated third parties. The Chamber believes that this approach is wrong, as it profoundly alters commonly accepted business practices. The definition of covered information is extremely broad as stated previously and includes several largely anonymous types of data, including cookies, IP addresses, and unique identifiers for computers or devices. These types of data points are inherently neither personal nor sensitive in nature and, thus, should not be subject to the strictest consumer consent requirements. Current regulatory requirements subject only the most sensitive data categories to an opt-in requirement, and many of those provisions recognize a lower standard when that data is used for marketing or advertising purposes. Furthermore, the exceptions for disclosure seem too narrow. It appears that the only allowed disclosures of non-employee information are those that are legally required. However, many companies with strong disclosure protections also allow limited disclosures for safety or health reasons, like product recalls, or when the company is a victim of a crime.

It should also be noted that the definition of sensitive information is overly broad and could, for example, be interpreted to expand the definition to include self-reported financial and health information in survey data. Additionally, as noted below, if this draft legislation would create a second layer of data regulation, then there could be significant conflicts in statutory regimes between this bill's provisions and those of existing federal laws such as HIPAA or Gramm-Leach-Bliley. Such a result may leave many businesses in the untenable situation of being unable to comply with two separate federal data privacy laws for the same covered information.

Greater Latitude Should Be Granted for Self-Regulation

Numerous industry self-regulatory programs exist today requiring that information used for marketing or advertising purposes be subjected to robust consumer notice and choice requirements. The following have provided such guidance: 1) the Direct Marketing Association; 2) the Network Advertising Initiative; 3) the FTC, which published self-regulatory principles; and 4) a joint effort led by five marketing industry associations—the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, the Interactive Advertising Bureau, and the Better Business Bureau—that published "Self-Regulatory Principles for Online Behavioral Advertising." These industry groups condition membership on compliance with their self-regulatory practices and sanction members who fail to comply. Self-regulatory practices promulgated by these industry groups or the FTC should be granted "safe harbor" status along with the concepts outlined in the law specifically for "network advertisers."

In addition, the draft does not address Web site browser controls, which are the paramount forms of online activity self-regulation today. Browser companies have increasingly developed their privacy-protecting user toolsets, and in recent years have begun to market these privacy differentiations to increase consumer use of their software. There is also a burgeoning privacy-by-design business model being developed using "plug-ins" and other tools to give browsers more privacy features and user controls. Increasing emphasis should be given to this self-regulatory vehicle. However, this draft would curtail the incentive for innovation regarding these browser controls.

Definitional Inconsistencies and Suggested Clarifications

Several definitions as currently drafted are either too narrow or too broad, and as constructed might unintentionally include many legitimate business practices that should not be covered by this draft legislation. The Chamber recommends revising the definitions of the following terms to ensure that the legislation sufficiently covers present day business practices:

- The definition of "render anonymous" exceeds practical use since it would apply to any "computer or device," which would restrict all forms of Web site analytics, market research, or other commonly anonymous uses of information. In addition, it would exceed the anonymization efforts governing "protected health information" under HIPAA which seems to be a contradiction in scope when comparing website use of personalized and protected health information. The Chamber recommends harmonizing the "render anonymous" definition with HIPAA's existing de-identification standard such that compliance with a similar de-identification process would provide a similar exclusion from this legislation.

- "Covered entity," "service provider," and "unaffiliated party": As drafted, it is possible for one entity to meet the requirements of all three definitions, thereby subjecting it to a number of different compliance obligations. The Chamber recommends carefully re-working these definitions such that there is no overlap or conflicting requirements for the same collection and use of covered information.

- The "advertising network" definition refers to "individuals," yet there is no definition of "individual" that would include a "unique identifier." As a result, few if any ad networks actually have "individual" information but rather cookies that are associated with a browser, which could be shared with a household or public network like a library or cybercafé.

- The definition of "operational purpose" should be expanded to include "detecting, preventing, or acting against actual or suspected fraud targeting the individual." Fraud detection products and services should not be restricted in this bill. This definition should also include market research.

- The definition of "transactional purpose," by specifically excluding marketing, advertising, and sales, prevents practices such as a customer being recommended

a certain book or album based on previous purchases, without a notice and opt-out. Marketing efforts designed to encourage transactions or sales should be considered as part of a transactional purpose and the definition should be expanded to include such purposes.

- The definition of "unaffiliated party" allows for sharing of information without opt-in consent as long as there is corporate ownership or control. The definition should also include entities that operate websites as joint ventures.

- The definition of Sensitive Information should be changed:

    - "Race or ethnicity" could cover ads delivered in different languages
    - "Mental or physical condition" is overly broad and could encompass common ailments, such as a stomach ache. The definition should relate a specific diagnosis.

Undefined Terms

The Chamber suggests that additional terms be defined to provide greater clarity and to ensure against inconsistent interpretations of their meanings, as follows:

- "Affiliates," "first party," and "third party": Further clarification on what is meant by first- and third-party entities will help industry better comprehend who is meant to have the various notice and choice obligations found in the bill.

- The terms for "consent," "opt-out consent," "express consent," "affirmative consent," and "express affirmative consent" are not defined. It is unclear how a compliant business would be able to understand and differentiate these terms when applied to data collection and use.

- The term "individual" should be defined to cover natural persons in the United States who are customers or visitors to online or offline channels where covered information is collected, and exclude employees, companies, and other persons or entities not intended to be covered.

- "Material change" in privacy practices is not defined, and it is unclear how it could be applied in cases where traditionally non-personal information uses as defined under "covered information" could be applied, such as with IP addresses or cookies where notice to these users is typically unavailable. It is unclear when or how an opt-in would be required and delivered, particularly for aspects of a policy where choice is not offered to begin with.

- There is no definition of "all or substantially all of an individuals' online activity." It is unclear whether this section is directed to Internet service providers, advertising networks, Web analytics providers or other entities. The legislation should clarify what is the perceived threshold for "substantially all."

The Chamber also recommends such a definition exclude fraud prevention and market research services.

Data Retention Language

The Chamber has concerns with the data retention provisions in Section 3(e)(2). If covered information is collected and/or used for multiple purposes, including transactional or operational purposes, it is important to know whether this section applies. Also, there seems to be a conflict between the deletion/anonymization requirement of this section and Section 4(b)(C), which protects against the alteration or destruction of covered information. In addition, where the user is in control over his or her own information (such as account data or transaction history) through a direct relationship with a provider, retention limits appear unnecessary and counterproductive.

Location Information

Precise geographical information should not be codified into law at this time as sensitive personal information. Instead, the Chamber recommends that the collection and use of this data be governed by self-regulatory models at this time. This is a rapidly evolving technological field, which could ultimately be helpful in such areas as fraud detection. Therefore, the Chamber believes that this type of information would best be left to a more flexible framework with guidance from the FTC.

Aggregate or Anonymous Information

The Chamber agrees with what appears to be the general intent of Section 5 of the proposed draft to exclude from the draft bill's notice and choice provisions the collection, use and disclosure of aggregate information or information that has been rendered anonymous. However, it is unclear how Section 5, as currently drafted, would function, and therefore requires further clarification. Additionally, it appears that the definition of "render anonymous" may be constructed too narrowly to cover the various methods by which personal information may be de-identified prior to use so that it is subject to this exclusion. As noted above, the Chamber believes it would be important to harmonize this provision and applicable definitions with similar safe harbors in other federal privacy laws, such as HIPAA's de-identification standard.

Modification to Section 7 Report

The Chamber recommends that the report in Section 7 not be limited to the Federal Communications Commission (FCC) alone, but instead should include the FTC as well. There are myriad privacy-related laws that exist today that should be more closely studied to better assess the impact that this legislation would ultimately have. It would be prudent for the implementation of the proposed regulations in this draft to only take place after these reports are received and reviewed effectively.

Competitive Neutrality

The draft potentially subjects different entities involved in online behavioral advertising to different types of notice and consent obligations, depending upon the type of business model they employ. For example, if a covered entity collecting information via the Internet posts its privacy notice "on the website" through which it collects information, it can avail itself of opt-out notice for the collection and use of covered information. While this approach may be workable for companies engaged in the "cookie-based" online behavioral advertising business models, it is unclear how it would apply to entities that may not (presently or in the future) rely upon visits to websites to collect data. Likewise, the draft allows entities that construct and maintain user preference profiles to utilize opt-out consent for the collection and use of covered information, but appears to preclude any new or different business models from doing so.

The draft should provide all entities involved in OBA with equal opportunities to utilize opt-out consent for the collection and use of covered information. It should not disfavor particular business models with more burdensome regulatory obligations, since doing so would deter entry, harm innovation, and undermine competition and choice in the OBA marketplace.

Conflicts with Other Federal Privacy Laws

The Chamber agrees with what appears to be the intent of the provision in Section 11 stating that this bill should have no effect on activities covered by other enumerated federal privacy laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and HIPAA. As currently drafted, however, the opening clause of the proposed legislation would create a significant exception to this general rule (i.e., by stating "except as provided in this Act"), which could be interpreted by the FTC or by courts to imply that this legislation would create another layer of regulation in addition to provisions in each of the enumerated acts. Given the potential conflicts with having the same type of data collection and use covered by more than one federal privacy regime, a covered entity could very well find itself unable to comply with two separate federal privacy laws for the same covered information, thereby involuntarily subjecting itself to fines and other enforcement actions for non-compliance with one or both of the acts. To avoid this potential conflict with existing federal privacy regimes, the Chamber strongly recommends that this section of the proposed bill be clarified to provide an explicit carve-out from the definition of covered entity for entities already covered by the enumerated acts.

Exemption for Publicly Available Information

The Chamber strongly believes that this bill should explicitly exempt publicly available information from the definition of "covered information." By definition, publically available information is not private. Information that is already in the public domain should not be covered by the bill. Moreover, this type of information cannot be used for identity theft purposes or any other nefarious activity, so its inclusion in this bill is unnecessary and should be explicitly left out.

Exemption for Employee Information

Similar to the previous comment, the Chamber strongly believes that employee information should be excluded from coverage by the proposed legislation as this information, while confidential to the employer and employee, must not be subject to an employee's choice to prevent its collection by the employer. Not only are employers required under federal tax and other laws to collect much of the data that would meet the definition of "covered information" in this draft bill, there are numerous existing federal and state laws that already protect the privacy and security of such employee information, not to mention court decisions that have sought to strike the proper balance between employer and employee rights to the information. It would be well beyond the stated purpose of this bill to re-write the laws on employer/employee data collection and use. Moreover, if employee information were to be covered, the proposed legislation would arguably affect nearly every employer in the nation, including the smallest of commercial entities, forcing them to modify employee data management practices. Therefore, the Chamber strongly recommends that the definition of "covered information" include an exclusion for information collected from or about a former, existing or prospective employee by an employer.

The Chamber thanks you for the opportunity to weigh on this draft bill and looks forward to working with you and your staff on this very important issue.

Sincerely,

R. Bruce Josten

Cc: The Members of the Subcommittee on Communications, Technology and the Internet

Mr. RUSH. Mr. Zaneis, please 5 minutes now.

STATEMENT OF MIKE ZANEIS

Mr. ZANEIS. Thank you. I used to work for the U.S. Chamber of Commerce, but I don't think they would appreciate me delivering their testimony here today. Thank you, Chairman Rush, Ranking Member Whitfield, members of the Subcommittee for holding this hearing for the opportunity to testify about these important legislative proposals. My name is Mike Zaneis, and I do work for the Interactive Advertising Bureau as Vice President of Public Policy.

The IAB represents some 460 companies involved in online advertising. Our companies run the gamut from the largest portals and search engines to branded publishers. It includes ad networks all the way down to the smallest Mom and Pop shop publisher online. The common theme for all of these folks is that they depend upon online advertising. It is a good industry and we are—continue to grow even in these tough economic times. In the first quarter of this year online advertising revenue in the U.S. grew to $6 billion. And that represents a 7.5 percent increase over the first quarter of 2009. More importantly, our industry is a major component of the national economy. We add more than $300 billion to the U.S. economy and provide more than 3.1 million jobs total.

But we know it is not all about economic numbers here today. We know in our industry that the number one asset that any company has is the consumer relationship in building trust through protecting their privacy and meeting their privacy expectations. That is why our industry has a long successful history of strong self-regulation. It began over a decade ago with input from the Federal Trade Commission when industries stood up to network advertising initiative. And this was a program to oversee third party ad networks and how they have collected and used data for consumers and provided choice.

But we knew over time as our industry grew and innovated then so too did our self-regulatory programs. They needed to innovate, and grow, and expand. That is why over 2 years ago IAD joined with the Association of National Advertisers, the American Association of Advertising Agencies, the Direct Marketing Association and in conjunction with the Council of Better Business Bureaus, one of the most respected, reputable self-regulatory monitoring and compliance programs in the world, to create for the first time a broad comprehensive set of online privacy practices for advertising purposes.

Here, too, we took away lessons from the Federal Trade Commission. They issued their staff report about online behavioral advertising privacy principles in February of '09. We incorporated many of those principles in our draft—excuse me—in our final principles that were issued in July of last year, including transparency, consumer notice, and something that we haven't talked about which is consumer education, which is really a key component here.

All of this leads me to the bills and the legislative proposals that are on the table today. And Mr. Chairman, I want to thank you for your recognition in H.R. 5777 about the importance of industry self-regulation. We think that that is the right approach in that it has a long history of success, it can be more flexible and dynamic,

and there is a commitment by industry and government agencies to make sure that it works. And we stand ready to work with you to make sure that any legislation that moves forward reflects upon and bolsters the success that not only the FTC has pushed out there and achieved, but in industry and our cross-industry self-regulatory group. We are beginning to see fundamental change online already in this marketplace about how consumers receive information about how data is collected and used, and pushing choice out ubiquitously.

That leads me to my second point that we are very gratified to see your recognition in the bill that a one size fits all consumer noticed jammed down in a privacy policy often is written in legalese may not serve consumers all that well. In fact, in our industry we are seeing a tremendous amount of innovation in better ways to serve notice to consumers and we hope to preserve that type of flexibility with any legislation that moves.

But—and there is always a but—we do have a number of reservations about H.R. 5777 and Congressman Boucher's proposal. And they share a couple of components that I would like to just identify here. The first is the concept that first party data usage requires an opt-out. Here we simply have to agree with the Federal Trade Commission's finding in their staff report. When consumers go to an online Web site they understand there is going to be a certain amount of data exchanged by that first party site and to serve them content and services and yes, advertising. And so, we think that they should be first party—clearly first party usage should be exempted out of this choice mechanism. Not notice—we should always do better around giving consumers notice about how the data is collected and used.

The second issue I would like to raise with you is the third party data sharing provision. The Internet is nothing but a series of third party relationships. Virtually every Web site requires these third party data sharing whether it is to customize content, to run your analytics on the back side to make sure you know who is coming to your site and who—and getting paid, or whether it is for relevant advertising. And so here again we agree with the FTC's principle in their staff report that you should have an opt-out requirement empowering consumers to exercise their choice when they have ligament concerns around privacy. You need to give them good notice, you need to empower them, and you need to educate them which is something that the IAB is committed to.

So I will just sort of leave you with this last thought and I look forward to your questions. I think it is impossible to take information out of the information age, because if you do that is what you are going to get is less relevant advertising, and less relevant advertising by definition is spam. I don't think anybody wants that. That is not good for consumers, and it is not good for business. Thank you.

[The prepared statement of Mr. Zaneis follows:]

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

HOUSE ENERGY AND COMMERCE COMMITTEE

HEARING ON

H.R. 5777, THE BEST PRACTICES ACT, AND A DISCUSSION DRAFT OF REPS. BOUCHER AND STEARNS TO REQUIRE NOTICE TO AND CONSENT OF AN INDIVIDUAL PRIOR TO THE COLLECTION AND DISCLOSURE OF CERTAIN PERSONAL INFORMATION RELATING TO THAT INDIVIDUAL

JULY 22, 2010

TESTIMONY OF

MICHAEL ZANEIS
VICE PRESIDENT OF PUBLIC POLICY

INTERACTIVE ADVERTISING BUREAU

I. Introduction

Thank you for the opportunity to testify at this hearing of the House Energy and Commerce Committee's Subcommittee on Commerce, Trade, and Consumer Protection. I'd like to thank Chairman Rush and Ranking Member Whitfield for holding this important hearing.

My name is Michael Zaneis and I am the Vice President of Public Policy for the Interactive Advertising Bureau (IAB). The IAB is the trade association for ad-supported interactive media in the United States. IAB's 460 member companies account for 86 percent of the interactive advertising sold in the United States. Our members include the great names of the online and offline media world – AOL, CBS, Google, MSN, The New York Times, Time Inc., Walt Disney, and Yahoo! among them – as well as scores of smaller publishers, advertising networks, and specialists in such areas as digital video advertising and mobile advertising.

IAB and our member companies vigorously support strong protections for consumer privacy rights and expectations in all media, online and offline. Delivering advertising relevant to users' interests and needs enhances their online media experiences and productivity, and helps businesses to grow. Those goals are not only complementary, but necessarily conjoined: Providing consumers with control over their online experiences has been a core principle of interactive media, commerce, and advertising from the birth of the medium. Moreover, reinforcing consumer trust in the medium is necessary for our continued viability. These principles – consumer control and trust – have fueled the Internet's growth into the most popular entertainment and information medium in the United States, and our emergence as the fastest-growing advertising medium in the World.

II. Self Regulation Is Robust and Effective

IAB strongly supports industry self-regulation and leading business practices as the most effective framework to provide transparency and choice to consumers. Such a framework will nurture the continued development of innovative offerings online. To this end, we believe that self-regulation inherently possesses features that make such an approach more effective than any legislation that might seek to govern the online ecosystem. Entities and their associations are best situated on the frontlines to interface with consumers and evaluate their experiences online. In response to any harm that consumers may experience, industry is uniquely positioned to respond swiftly to rapidly evolving online technological advances and consumer expectations with self-regulatory programs and best practices that carefully balance restrictions on the use of information with the significant benefits that such uses provide to consumers. Unlike self-regulation, legislation runs the risk of codifying outdated practices for decades to come whereas best business practices and self-regulatory programs can quickly evolve to address the dynamic online environment.

Industry has ample experience and a strong track record of navigating and promoting best practices online that provide for a variety of effective choices to consumers. These practices have been embodied in numerous self-regulatory frameworks in both the advertising and online privacy arenas. Among the most successful examples of effective self-regulation are guidelines and standards of organizations including the Council of Better Business Bureaus' National Advertising Review Council, the Direct Marketing Association, the Network Advertising Initiative, TRUSTe, the AICPA's WebTrust, and BBBOnline. These organizations and programs have many years of experience in developing flexible and effective best practices and standards that protect consumers' privacy online.

As a recent and very important example, in July 2009 IAB partnered with the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, and the Council of Better Business Bureaus to develop robust self-regulatory
principles that provide enhanced transparency and consumer control in online behavioral advertising.[1] We provided the Subcommittee with a copy of the Self-Regulatory Principles for Online Behavioral Advertising upon its release. Since that time, the associations have been working to implement these principles, placing a significant focus on providing enhanced notice to consumers in the form of an industry-developed icon and wording that will be used to demonstrate adherence to the industry principles for online behavioral advertising.[2] There have been tremendous developments in this area and any legislation should encourage such efforts, and not limit their development.

Self-regulation in the online behavioral advertising arena has been recognized by the Federal Trade Commission ("FTC" or "Commission") as the correct approach in this area. The Commission reached this conclusion after several years of focused study in the area. In the Commission's February 2009 Staff Report on Self-Regulatory Principles for Online Behavioral Advertising, the Commission indicated that "[s]taff supported self-regulation because it provides the necessary flexibility to address evolving online business models."[3] To this end, the report continued on to note that "in issuing the proposed Principles, staff intended to guide industry in developing more meaningful and effective self-regulatory models...."[4] The principles that IAB and the associations have set forth in the Self-Regulatory Principles for Online Behavioral Advertising are consistent with the framework espoused by the Commission and the timeliness of their release demonstrates industry's commitment to serving as a responsible actor online.

---

[1] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, Self-Regulatory Principles for Online Behavioral Advertising (July 2009), available at http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

[2] Press Release, IAB and NAI Release Technical Specifications for Enhanced Notice to Consumers for Online Behavioral Advertising: Critical Step in Interactive Industry's Ongoing Self-Regulatory Efforts (Apr. 14, 2010), available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041410.

[3] FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising, at 11 (February 2009) (hereinafter Staff Report), available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[4] *Id.*

III. Interactive Advertising Is Important to the U.S. Economy

As the FTC stated in its Staff Report, "Consumers have genuine and legitimate concerns about how their data is collected, stored, and used online. They may also benefit, however, from the free content that online advertising generally supports, as well as the personalization of advertising that many consumers appear to value."[5] Indeed, the scope of that value is breathtaking.

Interactive advertising is responsible for $300 billion of economic activity in the United States, or roughly 2% of Gross Domestic Product, according to a study released last year by the IAB and undertaken by Harvard Business School Professors John Deighton and John Quelch, along with Cambridge, MA-based Hamilton Consultants. The study was designed to provide an impartial and comprehensive review of the entire Internet economy and answer questions about its size, what comprises it, and the economic and social benefits Americans derive from it.

Professors Deighton and Quelch found that the advertising-supported Internet employs 1.2 million people directly in jobs that build or maintain the infrastructure, facilitate its use, or conduct advertising and commerce on that infrastructure. Under the reasonable assumption that each Internet job supports an additional 1.54 jobs elsewhere in the economy, then 3.05 million, or roughly 2 percent, of employed Americans owe their employment to the advertising-supported Internet.

Internet jobs are widely dispersed across the United States. Every one of the 435 U. S. Congressional districts contains at least 17 Internet employees. Some districts support as many as 6,500, and twenty-four districts have at least 1,000 identified Internet employees.

For the 19 states represented on the Subcommittee, our industry contributes over $218 billion in revenue annually and is responsible for the employment of over 2.6 million people.

Some 20,000 small businesses operate on the Internet. The online auction site eBay alone is the primary source of income for 120,000 individuals who earn their living as sellers; another 500,000 men and women have part-time businesses on eBay. A 2009 *Wall Street Journal* report estimates that nearly half a million individuals may make their living as "bloggers," or small publishers of online content.

At work and at leisure, about 190 million people in the United States spend, on average, 68 hours a month on the Internet. This is unsurprising, for the Internet is a vast treasury of quality content, such as news, business information, entertainment, maps, and self-help resources. Education and information-gathering tools, including search engines, have undoubtedly democratized the availability and accessibility of educational content. The

[5] *Id.* at 7.

Web is a communications lifeline for an enormous number of people. There are an estimated 1 billion users of free email services worldwide. Some 100 million Americans keep in touch with family and friends through social networking sites. Last November, 124 million Americans viewed 9.5 billion videos online that were uploaded by others.

All of these services, information, and entertainment are free. Although, as you and I know, they are not really free: They are supported by advertising.

This is not surprising. From the early 19th Century, advertising has been at the center of a vital value exchange between businesses and consumers. We provide quality news, information, entertainment, and other services, in return for which consumers give us their time and attention. That time and attention, in turn, allows businesses to communicate the availability of goods and services to consumers and customers. Advertising is the heart of the U.S. consumer economy.

Given the centrality of the Internet to Americans' lives, it's natural that advertising has grown to become the medium's primary financial support. In 2002, advertising contributed 7 percent of the $78 billion paid for Internet services to the U.S. economy. In just seven years, while the value of the Internet has doubled, advertising has increased fourfold and its contribution to the pool of funding for the Internet has grown to 11 percent. Advertising is the only Internet funding source that has shouldered more of the burden than seven years ago. Online interactive advertising has substantially reduced what consumers have had to pay for e-commerce products and services.

IV. Regulation Presents Risks

The interactive advertising industry continues to grow and provide greater benefits to consumers. In the first quarter of 2010 alone, interactive advertising revenues in the United States hit nearly $6 billion. This shows a 7.5% revenue growth over the first quarter of 2009, despite a difficult economy, and at a time when overall advertising spending was decreasing.[6] You might think that a medium so wildly popular and so useful for so many people would be strong enough to withstand any and all challenges. But the interactive advertising ecosystem is fragile. In their report, Professors Deighton and Quelch caution against inappropriate "restrictions on advertising or use of individual-user data [which] could undermine the effectiveness of major elements of the Internet."[7] The components of the ecosystem that they believe could be compromised include:

- The ad-supported search engines and many content sites that provide information, entertainment, news, and social networking;

---

[6] Q1 '10 Internet Advertising Revenue Press Release, IAB Internet Advertising Revenue Report conducted by PricewaterhouseCoopers (May 13, 2010), available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-051310.

[7] Hamilton Consultants, Inc., with Dr. John Deighton, Harvard Business School, and Dr. John Quelch, Harvard Business School. Economic Value of the Advertising-Supported Internet Ecosystem, at 9 (June 10, 2009), available at http://www.iab.net/media/file/Economic-Value-Report.pdf.

- The enterprise websites created by companies and other institutions that increasingly are able to individualize the messages; and
- The e-commerce companies that use data to personalize offers to current customers.

As a representative of the interactive advertising industry, I too share their concerns. Some of the proposals we have seen from advocacy groups and the legislative proposals being considered today could unintentionally cause material harm to the existing interactive advertising industry, and impede our industry's growth and constrain the services and content that are currently provided to consumers, largely free of charge.

V. H.R. 5777 Represents Significant Progress in the Privacy Debate

A. Industry Self-Regulation Remains the Most Effective Framework for Protecting Consumers

I'd like to commend the Chairman for recognizing the value and importance of a strong self-regulatory program. As mentioned earlier in my testimony, industry has been working diligently these past twelve months to set-up a self-regulatory regime that encompasses the entire online ecosystem, from publishers to service providers. I'm pleased to see that some of the Principles first proposed by the FTC and subsequently adopted by the self-regulatory program are incorporated here in Title IV of H.R. 5777.[8] However, this is a complicated process and I believe that further refinements to the language can be made to make it compatible with the FTC's and industry's existing work.

I believe that the incorporation of Title IV in this legislation is truly a testament to the hard work and progress industry has made in this area. While I applaud the Chairman's inclusion of Title IV, I would like to briefly note some of the incredible complexities and unintended consequences that can arise when attempting to legislatively proscribe practices that do not conform to existing business models, and limit flexibility to develop new models.

As the online advertising business model currently exists, most advertisements being served on publisher websites are in fact being served by third party companies, such as ad networks. Third party ad-serving platforms, such as Doubleclick and Atlas, deliver almost 90% of the display advertisements seen online. Virtually all small publishers – the ad-supported sites and blogs too specialized to afford their own sales staffs – sell and place ads via online advertising networks like Burst Media and Advertising.com. Since these ad networks are largely responsible for the serving of ads that appear on publisher websites, and data collection, they are best situated to provide consumers with options

[8] Two key Principles of the Self-Regulatory Principles for Online Behavioral Advertising include Consumer Control and Accountability, which are both addressed under Title IV; §403, 1A references a "clear and conspicuous opt-out mechanism" (i.e. Consumer Control) and §403 2C acknowledges the realization that "accountability and compliance testing is important."

regarding notices of data collection as well as choices as to how that data is being used. However, as currently drafted, H.R. 5777 does not fully consider the role that these types of third parties play in the online advertising space, and instead focuses on data collection being done by a first party, i.e. a publisher.[9] This type of requirement does not reflect the true nature of how data is collected and used in the online marketplace. Given the incredible technological intricacies of the online advertising marketplace, it can be very easy to miss such seemingly trivial, but critical nuances.

B. A Flexible Notice Requirement Is Key for Keeping Consumers Informed and Engaged

It is no secret that it has become harder and harder to get consumers to pay attention to privacy policies. Privacy notices and policies seem to have proliferated in both the online and offline worlds over the past ten years, and industry has evolved to become increasingly more creative in catching consumers' attention. It would be fair to say at this point consumers are feeling inundated with potentially confusing privacy notices.[10] The presence of Section 102 (F) – that the FTC should consider "the risk to consumers and commerce of over-notification" – demonstrates that the Chairman is aware that this practice may not in some instances serve consumers well. We commend the Chairman for this recognition and believe that Title I of H.R. 5777 takes a progressive and innovative approach in recognizing that when it comes to privacy notices, one size does not necessarily fit all.[11] The FTC Report urged industry to seek ways to provide consumer notice outside of the privacy policy. This provision has been fully embraced by the cross industry self-regulatory group and we have established new and innovative ways to deliver more easily identifiable and understandable notice to consumers. I applaud the Chairman's inclusion of language that would allow for innovation in this area, giving industry the opportunity to do what the advertising industry does best – get consumer attention – and hope that as this draft is considered that it will move even further towards this flexible, effective standard.

VI. H.R. 5777 and the Boucher Proposal Could Limit Critical Existing Business Models

A. H.R. 5777 and the Boucher Proposal Impact the Relationship Between First-Party Publishers and Their Customers

---

[9] Title IV, §403 1A, as drafted, appears to only cover the transfer of data from a "first-party" (i.e. publisher) to a "third party" – it does not appear to cover scenarios where a third party (i.e. ad network) is collecting the data.

[10] A bill currently in the Senate Committee on Banking, Housing and Urban Affairs entitled the "Eliminate Privacy Notice Confusion Act" (H.R. 3506) would amend the Gramm-Leach-Bliley Act to provide an exception from the continuing requirement for annual privacy notices for financial institutions in limited circumstances. One of the rationales behind the bill has been that consumers are becoming desensitized to privacy policy notices.

[11] §102 (b) of Title I, "Provision of Notice or Notices" allows for the FTC to promulgate regulations that would allow for variations in how notice could be delivered, i.e. variations based on type of media being employed, whether a short notice or limited disclosure would be more appropriate, etc.

H.R. 5777 and the Boucher proposal both envision imposing opt-out requirements on first parties that would impact the relationship between customers and publishers. Consumers are aware of, and significantly benefit from, use of information from first-party sites. Many consumers also enjoy personalized webpages when they return to a website with which they have had a previous interaction and perhaps an ongoing relationship (*e.g.*, personalized websites for consumers that frequent online retail ecommerce sites). People visit such sites with the expectation of exchanging information in order to benefit from the sites' online offerings.

When the FTC first began exploring the issue of how first parties should be treated in the online behavioral advertising context, it initially proposed a similar standard to the one set forth in H.R. 5777 and the Boucher proposal.[12] After reviewing feedback on the proposed principle, however, the Commission determined that the principles should exclude first parties and avoid getting in the middle of first parties and consumers.[13] The FTC reasoned that "'first party' behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm"[14]and that "given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it.[15]"

I encourage the bill sponsor to adopt language in this area that incorporates the FTC's findings and allows the first-party/consumer relationship to remain strong and vibrant. This principle could, for example also be included within the self-regulatory provisions of the bill.

B. We Support Applying an Opt-Out Standard to Sharing with Unaffiliated Third-Party Publishers

H.R. 5777 and the Boucher proposal would impact online information flow by restricting transfers of information to unaffiliated third-party publishers. IAB members have long adhered to the principle of providing choice to consumers through opt-outs for the transfer of data to third parties for advertising and marketing purposes. We believe that such a standard is critical any legislation in this area.

As recognized in the Executive Summary of the Boucher proposal, online advertising supports much of today's online commercial content, applications, and services that are available for free. In addition, Congressman Boucher has many times publically stated that consumers generally do not "opt-in" or "opt-out" of information sharing and advertising. In the experience of our members, only those few individuals, sometimes called the "privacy fundamentalists," opt-out. Thus, requiring consumers to opt-in to

[12] See FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising (February 2009) (hereinafter Staff Report), available at http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf.
[13] *Id.* at 46.
[14] *Id.* at 26.
[15] *Id.* at 27.

transfers to third parties would drastically reduce the free flow of information that is the heart and soul of today's Internet offerings. Currently, information is collected in a seamless manner that does not interrupt a consumer's online experience. Changes to the system proposed in H.R. 5777 and the Boucher proposal would turn the Internet from a fast-moving information highway to a slow-moving toll-road. Such a move would hinder, not facilitate ecommerce. We stand ready to help craft a consumer choice standard that would preserve this important source of revenue upon which the Internet depends.

C. The Scope of "Sensitive Data" in H.R. 5777 and the Boucher Proposal Is Too Broad

We have reservations about the broad scope of the term "sensitive information" contained in these legislative proposals. The proposed definition extends beyond the data identified as sensitive by the FTC.[16] We can all agree that subsets of the enumerated areas should be subject to heightened standards. However, this is a complicated area that should be studied and requires further refinement.

This provision would restrict multicultural marketing and media. The definition of "sensitive information" includes online communications to ethnic, racial, and religious minority audiences and places an opt in requirement for marketing to these audiences. Latino, African-American, and Asian-oriented Web sites would certainly be prevented from providing media kits to or delivering customized content or advertising on behalf of the agencies that place ads on their sites. While certainly not intended, we are concerned that these types of services provide great benefit to these audiences and the proposed restrictions would unintentionally harm the very groups of people they seek to protect.

D. H.R. 5777's Private Right of Action Is Unnecessary

We are very concerned with H.R. 5777's inclusion of a statutory private right of action in this area. I am not aware of any instances of a consumer being economically harmed by the collection or misuse of any data collected for online advertising purposes. The chilling effect on legitimate commerce in this area that could result from a private cause of action should not be overlooked.

Title VI of H.R. 5777 allows for multi-enforcement efforts by both the Federal Trade Commission as well as state attorneys general. Given their extensive expertise and experience in investigation and enforcement, the FTC and state attorneys general are well-positioned to handle any potential complaints. In particular, the thousands and thousands of small and medium-sized websites that don't have the capacity to deal with the uncertainly and expense of defending themselves against a barrage of lawsuits that may be meritless.

---

[16] *Id.* at 43-44.

E. An Access and Correction Regime Is Unwarranted In This Environment

Given that online advertising data is largely anonymous in nature, a legislative standard calling for "access and correction" databases is both unnecessary and workable. Unlike information governed by the Fair Credit Reporting Act, data being used for online advertising purposes is generally information that involves clickstreams, cookies, dynamic IP addresses – essentially, pieces of information that amount to long streams of text or code that aren't identifiable to an individual. They don't include names, addresses, social security number, financial account numbers, balances owed, credit limits, etc. Most third parties in this ecosystem do not know what individual is associated with a certain cookie or clickstream – pragmatically speaking, if they cannot identify an individual, they cannot offer opportunities for access or correction to information about that individual. Thus, this provision would unintentionally create a perverse incentive for companies to collect more personally identifiable information than they currently do in order to comply.

Setting aside these pragmatic concerns for a moment, another question raised by the access and correction language in H.R. 5777 is the question of what harm is possible based on an online marketer, publisher, or network collecting clickstream data about the fact that a consumer likes blue shirts vs. red shirts. While the access and correction language included in Title II of H.R. 5777 may serve a demonstrable purpose in other regimes, where misuse of information could result in an individual may being denied employment or access to credit, we are concerned that it is an overly burdensome standard in the collection and use of data for online advertising. The use of information for making critical determinations such employment or credit are already strictly governed by other laws. If there are similar potential misuses of information that necessitate such a standard, these uses should be specifically enumerated and considered on their merits rather than such a general requirement that would impact so many millions of businesses of all sizes.

VII. Conclusion

Thank you for considering the views of the IAB on these issues. The success of the Internet has helped fuel this country's economy and it is important to ensure that this medium can continue to grow and thrive. We look forward to working with members of the Subcommittee as they consider privacy proposals and the legislative process moves forward.

Mr. RUSH. The Chair wants to thank all of the witnesses for your outstanding testimony today. A vote now occurs on the floor of the House of Representatives. There are two votes—should be probably about 30 minutes or more—around 30 minutes, so it is the Chair's intention to recess the Subcommittee and to reconvene immediately after the last vote takes place. So it will be about half an hour. So I apologize for the interruption of this hearing, but we will be back as soon as we can. The Subcommittee now stands in recess.

[Recess.]

Mr. RUSH. The Committee will reconvene, return to order. The Chairman recognizes himself for 5 minutes for the purposes of questioning the witnesses.

Mr. Hoffman, I was interested in your testimony, and in your testimony you highlighted the importance of providing FTC rulemaking authorities to flesh out certain requirements in the Best Practices Act and to adapt the bill's provisions to changes in technology. Other stakeholders have raised concerns that providing FTC with this type of rulemaking authority in the bill will create enormous regulatory uncertainty that is bad for commerce.

What are your thoughts on this? If FTC does not provide a rulemaking authority, will the bill quickly become outdated? Are you concerned about regulatory uncertainty and would you answer those questions for me, please?

Mr. HOFFMAN. We think the Best Practices Act does an excellent job of not just providing rulemaking authority to the FTC, but guiding that rulemaking authority by certain criteria that should have to shape the regulations that would emanate from the FTC. Our perspective when we look at privacy legislation is to allow privacy to continue to actually aid innovation instead of impede innovation.

Individual pieces of legislation need to be technologically neutral to allow for the enforcement agencies to apply those principles to the individual new business models when they come up and to provide guidance in that way. The FTC has been an absolute leader in doing that for the past decade.

Mr. Vladeck mentioned the various methods that they have used to do that with the different enforcement actions that they have taken, plus the round tables that they have held, and how they have communicated with industry and academics. We think that the Best Practices Act balances those different interests very well.

Mr. RUSH. Ms. Harris, is the importance to FTC rulemaking the—in this act just for consumers and is it just for business also?

Ms. HARRIS. We think so. You are always—when you are writing a bill like this you can be highly specific, and the bill will lock in today's business practices, it will not have the flexibility that you need for business practices that we haven't seen, and it will not allow the law to basically live in a way that will address business practices we haven't seen. Giving the FTC very specific rulemaking authority here first of all allows them to take into account the different kinds of business models and technologies that we are dealing with, but it also, I think, allows over time for modifications depending on changed circumstances. So yes, we think FTC rulemaking is essential here.

Mr. RUSH. In past legislation the third party or unaffiliated party has been defined based on the corporate structure of an entity, such as common ownership or corporate control. And during this hearing and in other sidebar conversations we have heard concerns that consumers may not understand which entities are subsidiaries, affiliates, parent corporations, or otherwise under common control with another company. On the other hand, corporate structuring is known and we do not know—we don't want to draw an arbitrary line.

Ms. Harris and Mr. Mierzwinski, do you believe that consumers may have difficulty understanding when entities are related by common ownership or control? Should privacy matter? Should privacy legislation take into account the best reasonable expectations of the consumer as this act does? And is this a workable definition? Lastly I—you can answer these three questions in the manner that you would choose to. Lastly, what are the benefits of an approach based on common ownership or control and does it provide companies with more clarity? Those are a series of questions. I hope you can kind of summarize the questions in your answers.

Ms. HARRIS. I am going to let Ed go first.

Mr. MIERZWINSKI. Oh, thank you, Chairman Rush, and I think I want to commend you on your provision recognizing the artificial distinction of this corporate common control. Consumers don't have any idea that their bank owns some hundreds or thousands of other affiliated entities. And the Internet has a number of networked companies that are the same way. So going to an activities based definition rather than a corporate ownership definition, we support that, and I think it is much closer to consumer expectations that except for the company you are doing business with, pretty much everyone else is a third party.

Ms. HARRIS. So I generally agree. I do think that your bill probably gets it as close to right as you can because it is a complicated issue. I am glad that there is some room for FTC rulemaking on that provision. The key question here is would a consumer under reasonable circumstances believe that they are dealing with an entity that is under common control. And I really think that that is probably—has to do with common branding. I think most of us know that GAP and Banana Republic and Old Navy and a whole set of companies are sort of one. But given a sort of large multinational that owns many, many, many different lines of business, we have to keep that very narrow in the interest of the consumer and I think you've done that.

Mr. RUSH. The Chairman's time is concluded. Now the Chairman acknowledges Mr. Whitfield for 5 minutes.

Mr. WHITFIELD. I thank all of you for your testimony and trying to balance protecting privacy versus generating revenue for advertising to keep the Internet the vibrant marketplace that it is—searching browsing history of a particular person, and can some of you, maybe Ms. Harris or Mr. Mierzwinski, identify for me the privacy concerns with the anonymous monitoring of web browsing history, and should that require the same level of consent as using information like Social Security number, bank account numbers and so forth, and just give me your perspective on the differences therein.

Ms. HARRIS. Mr. Whitfield, the way that they are able to collect discrete pieces of browsing history is usually to tie them together with an IP address. In that instance companies can pull them together into profiles, and they can be put together with information to identify the consumer. So in the technological environment that we are in now, the ability to bring discrete pieces of information together into an identifiable profile is simply much easier. I think that there is a conversation to be had wherein where you draw the line and—but I think that that is something that has changed dramatically from, you know, the first time that privacy legislation was introduced in Congress.

Mr. MIERZWINSKI. Mr. Whitfield, I would agree and I would say that from my perspective one of the strongest pieces of both bills is that IP addresses insensitive information. We are concerned that de-identified or supposedly anonymous information can be repackaged back together. There are numerous examples of that happening, and I would also point out that a recent complaint by U.S. PIRG, the Center for U.S. Democracy, and other groups talks about just how easy it is and how the technology has changed in the last few years that consumers are being sold on a real time basis now. They are not compiling dossiers that take even half an hour to compile. The ads are being served instantly. They are being brokered to the highest bidder. It is very sophisticated, and little bits of information can add up very quickly.

Mr. WHITFIELD. Mr. Zaneis, would you like to comment on this?

Mr. ZANEIS. Yes, thank you very much, appreciate the opportunity. I think Congress has to be careful not to try to legislate the possible, or the theoretical, and to understand the business model. And here I actually disagree slightly with Leslie. It is not that VAS or predominant business model to tie click stream data back to personally identifiable information—certainly not in the online advertising space. In fact many of the ad networks specifically—advertising networks deliver some 90 percent of all ads online. They are generally third part by nature. Their business model generally is not to try to tie it back to what we would traditionally think of as personally identifiable information. Certainly there is a lot that is possible through technology, but I don't think we can legislate the possible. We ought to be looking at actual business models, and I think that when we look at H.R. 5777 it actually gets closer under their definition of covered information to what we ought to be focusing on, which is things that are actually personally identifiable, not sort of anonymous in nature.

Mr. WHITFIELD. And Mr. Rubinstein, since you are an academic here, do you have any comments on this? We always value academics' thoughts.

Mr. RUBINSTEIN. Thank you, Mr. Whitfield. I would think I would just add that it is important not to think of anonymous data as just a binary category, that it is—data is either anonymous or it is not anonymous. And the emphasis might be on specific context, so how much data is being assembled and what is the quantity of data? Is it being publicly shared or privately shared? What is the specific context? Rather than try to get at this through definitions that have just a black and white aspect to them.

Mr. HOFFMAN. I would just like to add one point on that—to that. I think the current draft of the Best Practices Act actually recognizes that reality that Professor Rubinstein is commenting on. As an employee of a technology company there are a number of unique identifiers in hardware and software that are used on most computing platforms. What is happening in reality—Mr. Zaneis' point is a very good one. We need to look at the realities. It is some of those unique identifiers that are used and apt to correlate to a lot of this data that could be described sometimes as personally identifiable information. Others might say no, it is only identifying a particular device or a particularly device at a point in time. That is why I actually think the definition of preference profile which is saying that it is a list of preferences associated with an individual or with an individual's computer or other device, but then tying that to allow exception for participation in a choice program is an excellent way to navigate the issues that even if something is not completely identifiable to a particular individual it still could have the great potential to impact an individual.

Mr. WHITFIELD. Thank you. I see my time has already expired.

Mr. RUSH. The Chair now recognizes Mr. Space.

Mr. SPACE. I won't need fifteen, Mr. Chairman. In fact, I won't even need five, but thank you. I really don't have any questions having come in after the votes and after the testimony, but I do want to express my appreciation to Chairman, and to the Ranking Member for the deliberate process that we have undertaken in examining, reviewing, and modifying issues relating to privacy when it comes to access to the Internet and broadband generally. I think that having all the stakeholders present and participating in this discussion is very, very important and we see that today. We have seen it in the past, and we will see it in the future whether it is academia, industry, govern officials, consumer advocacy groups—all of those stakeholders deserve a place at the table and our Chairman and the Ranking Member have offered them that.

So I want to thank the witnesses today, thank you, Mr. Chairman, and the Ranking Member for again such a deliberate a thorough analysis of an issue that is becoming increasingly important as we see the role of broadband integrated into virtually all aspects of our lives. And I yield back my time.

Mr. RUSH. The Chair thanks the gentleman for his kind remarks. And the Chair will now entertain a second round of questions, and with that in mind, the Chair recognizes himself for 5 minutes.

This question is addressed to Mr. Vladeck and Mr. Zaneis. Section 303 of the Act says some entities using covert information or sensitive information for any purpose for as long they are in—business or in law enforcement need. Is our rebuttal presumption—is it too vague? What would be wrong with setting a date certain restrictions say in six months or a year?

Mr. VLADECK. Mike, do you want to go first?

Mr. ZANEIS. No, you go ahead.

Mr. VLADECK. The Commission has not taken a position on any of these issues and we would like the opportunity to comment later on once we have had a fuller opportunity to look at this. Just generally, you know, we believe that certain kinds of information

ought to be subject to heightened protection. And so that is, you know, the Commission has made that clear in other context.

Mr. ZANEIS. We are going to figure this out. Luckily I represent the advertising industry so I know how to get my message heard even when people don't want to hear it. I think Section 303—I think one size fits all doesn't always make sense in the online space. What you see here is a diversity of opinions, but what we see in the industry is a diversity of business models. And sometimes they may need to keep information for different purposes, and what is a legitimate business purpose I think differs, so you know, I want to take that back to my members and see if it is something that they are going to be supportive of or if there is some refinements we need to make. But as we have seen around things like consumer notice and other areas, a one size fits all isn't always the best approach, but we are willing to look at that and work with the Committee and you, Mr. Chairman, on that.

Mr. RUSH. Mr. Rubinstein, would you chime in on this with your opinion, please?

Mr. RUBINSTEIN. I would generally agree that having different time periods for different types of data or different purposes is a good idea rather than a single limit. I think the one thing that Congress should worry about, though, is companies that would retain data simply because they might have some use of it in the future. So where it is that non-specific and it is just a future business possibility, I don't think that is a sufficient reason for some unlimited period of retention.

Mr. RUSH. Mr. Rubinstein and Mr. Mierzwinski suggested in their testimony that this safe harbor in H.R. 5777 in several ways. I am going to ask both gentlemen what specific recommendations do you have for structuring the safe harbor provisions?

Mr. MIERZWINSKI. Thank you, Mr. Rush. I think the bill as currently structured captures the key point that I emphasized about having a mix of carrots and sticks, and that the Private Right of Action serves as a very significant stick or incentive for businesses to join. I think the one thing that I would call attention to, though, is whether the safe harbor choice program has a strong enough emphasis on high performance standards. And that is why I emphasized data governance practices such as appointing a chief privacy officer or having privacy by design methodologies so that there are other standards that a choice participant lives up to which in effect entitles them to the exemptions that they enjoy under the choice program. And I think the question then is how to best balance that mix of exemptions on the one hand that serve as incentives to join while ensuring that only companies engaged in a very high level of privacy protection are then entitled. Finally I would point to the desirability having some form of public consultation as part of this process and one way to do that might be for a choice program as part of their application for approval to indicate what type of public consultation they have engaged in. Have they met with advocacy groups, have they met with the public, if so how have they addressed concerns that those groups have raised. If they haven't addressed them, why not. So that all is transparent and available to the FTC in making its evaluation of the choice program.

Mr. MIERZWINSKI. Mr. Chairman, I would add to that that I think our concern is that many self-regulatory programs whether under the Securities and Exchange Commission, whether under the FTC, or other agencies, they work best when they have a robust legal standard, robust statutory framework underneath. And relying on the companies themselves and rule making only by the FTC is usually not good enough. And we would urge you to consider strengthening the Federal Trade Commission's monitoring of the choice program and the accountability mechanisms in there. And to do that of course, we would also support strengthening the Federal Trade Commission in general if they need additional resources to do those kind of things.

Mr. RUSH. My time is up. The Chairman recognizes the Ranking Member.

Mr. WHITFIELD. Thank you. Is there anyone on the panel other than Mr. Goldman that believes there should not be private right of action? OK.

Mr. HOFFMAN. Intel does not support a private right of action. We think that it—in the context of privacy in the great percentage of situations the individual actually does not even potentially know that they have been harmed, and they don't know who actually has caused the harm until after. We think that the best use of resources is to focus on mechanisms like the choice program in a way that was just articulated. It really—to vote those resources to organizations putting into place robust accountability mechanisms into their compliance programs that way we will avoid the breaches before they even happen.

Mr. ZANEIS. And I won't take up much of your time. I couldn't agree more. I would just say then I think what we might want to focus on legislatively is strengthening the Federal Trade Commission and their enforcement, and more resources, more cops on the beat I think would be a good thing in this area.

Mr. WHITFIELD. I am certainly not an expert in this area. In fact, I am far from it, but I have read that the OECD's privacy protection rules, guidelines for privacy protection are some of the most stringent in the world. Is that your understanding as well—most of you? Do you understand that to be true?

Mr. MIERZWINSKI. I would just say it is—the understanding in privacy that they are the most robust implementation of the Fair Information Practices that were actually first developed by a U.S. Regulatory Committee, but how they are implemented in law is different in different places. And I would say the only U.S. law that comes close to implementing them in a very strong way is something called the Fair Credit Reporting Act which regulates credit bureaus. Other laws rely on a much weaker version on the FIPs.

Mr. WHITFIELD. Well, we—if we were to adopt the OECD principles basically would you support that or——

Mr. MIERZWINSKI. Oh absolutely, and I want to say that both bills adopt parts of it. And in fact the Best Practices bill adopts quite a bit of the Fair Information Practices. We think we can go further with purpose, specificity, data minimization, data retention, and again accountability that is giving more rights to the data subjects.

Ms. HARRIS. Mr. Whitfield, I just—I want to agree that a strong set of Fair Information Practices and certainly the OECD is sort of the foundational in the United States. The Department of Homeland Security issued a set a few years ago that I think are you know perhaps captures some of the more modern concerns just a little bit that basically the bill really needs to include them all. That we have spent a long time focusing on you know opt-in, opt-out consent from the consumer, and when that is all you have in a bill, then you are pretty much telling the consumer that they have got to figure it out. They have to read privacy policies, they have got to understand it, and that the companies don't have any substantive obligations. When you include data minimization, et cetera, then you are putting real limits and the companies have to decide how to handle those.

Mr. WHITFIELD. Mr. Mierzwinski—oh I am sorry, go ahead.

Mr. ZANEIS. Sorry, I just—I want to be sure that the Chairman and you, Ranking Member Whitfield understand that there is a lot of Fair Information Practices in—certainly in H.R. 5777. I—you are talking about notice, and choice, and data security, and accuracy. These are Fair Information Practice principles. That does not mean you need all of them in a bill about things like marketing databases. In our written testimony we go into the access and correction provisions and the reality there is what we are talking about in some of these marketing databases are strings, user agent strings which are nothing more than computers talking to computers telling you what for instance operating system a computer—a person is using to go to a site. This is used to render the content readable to the consumer. I ask you what is the, you know, what is the purpose in allowing correction to that type of database? It is gobbly-goop to the consumer, and I worry about allowing people to get into those databases when there is no real harm. We are not talking about Fair Credit Reporting Act. There you are talking about adverse actions against consumers, things centered around employment eligibility, access to credit, getting a home mortgage that is not what we are talking about here.

Mr. WHITFIELD. May I ask one other question?

Mr. RUSH. Ms. Harris wanted to respond.

Mr. WHITFIELD. Oh, I am sorry.

Ms. HARRIS. I want to strongly disagree with that. Access is one of the key Fair Information principles. The likelihood that a consumer is going to demand access to a string of code I think you know if that is the concern my guess is we can figure out how to handle it in this Committee. But we are building larger and larger databases with all kinds of information and to me that is one of the fundamental rights that consumers have and that it needs to be part of this bill.

Mr. WHITFIELD. In Mr. Rush's bill in the definitions under covered entity it simply says engaged in interstate commerce whatever, whatever, whatever, and since I was in the railroad industry I know that when we talk about federal preemption it is from the business standpoint. We always loved federal preemption because we had some certainty in whatever state we operated in and so forth. And I know that a number of you would be opposed to federal preemption in this arena. Are any of you opposed to—OK——

Mr. MIERZWINSKI. We are very strongly opposed and the Best Practices bill is a much narrower form of preemption, but we prefer that federal law be a floor.

Mr. WHITFIELD. What about you, Mr. Rubinstein? Do you have a comment on that?

Mr. RUBINSTEIN. I would favor a narrow form of preemption. I think that it does allow businesses to operate with more certainty, and it is extremely difficult, and costly, and not very effective to have to design compliance programs that vary depending on which state you operate in. So I think some form of preemption is a necessary aspect of this bill.

Mr. WHITFIELD. Did you want to make comment, Ms. Harris?

Ms. HARRIS. Yes, Mr. Whitfield, it is CDT's position is that first the bill has to be good enough at the federal level to consider preemption. So you know in saying whether we support it or don't support it you know this is a messy process. But assuming that the bill provides the right degree of protection then a narrow preemption that really covers just those covered entities and just those practices is something that we are comfortable with. But you know there is a threshold of what the bill is implying, and we do think that Mr. Rush's bill gets that right.

Mr. WHITFIELD. Yes, well I was assuming that if Mr. Rush pushed the bill through it would be all right.

Mr. RUSH. I want to get in on one of the questions, and this question is addressed to Mr. Goldman and Ms. Harris. In your testimony earlier you say that user ID's and implications alone should not be defined as covered information. And given the fact that there are software passwords, guessing tools out in the marketplace, what kind of concerns can we have? And I am kind of pointing to a recent development among myself and—with myself and some other members of Congress. There is a certain company that has something they call street maps and I am really alarmed by these street maps. My residence has shown up on these street maps, and there are other members of Congress whose residence has shown up on these street maps and we are concerned about the notability (ph) especially for us protecting—protecting assets to the webs and Internet. What kind of harm could be visited by consumers with some of these different programs and would you respond to that Ms. Harris and Mr. Goldman about these certain issues?

Mr. GOLDMAN. I think as in our testimony I think we talked about how if the information is not directly linked back to the individual, so if it is just a password or some other kind of information that is not, you know, connected to your other kind of personal information, that should not be part of the PII. And so I think that is where we are at. You know, you could—theoretically you could have a lot of information out there. There is a lot of information out there. You might, for example, if you belong to a social network, you know, a social networking site you might put your name up there, you might created a username. You know, but it might not be linked back to your own name, your own personal—I guess whether financial or health information. So I think you know, as long as that is—the question is what is going to harm us in result from all that I think. And as we go into—our testimony also talks

about we are hesitant about adopting sort of new standards and new definitions of covered information. I think you know to the extent that we can standardize definitions across, you know across bill, across state bills, and federal bills that would be a good thing. So if you look at personal information as defined in some of the state bills, some of the state data breach and privacy bills I think, you know we have not taken—I think there will be some support for that. But I have not talked to our members about that at all yet.

Mr. RUSH. Ms. Harris, you have a response?

Ms. HARRIS. If the question is about, you know, whether we should be covering passwords and unique identifiers that protect this kind of information then I think in the right circumstances we should and I think that your bill does do that.

Mr. RUSH. Does any other witness want to respond? Mr. Hoffman?

Mr. HOFFMAN. Yes, I think it is a very good question. I think we find ourselves in a situation where there are a number of different kinds of data that while they do not point to a very specific individual, they might point to a device or a location or something that could end up impacting that individual. This is a very difficult balance to sort out. I actually think the Best Practices Act comes very close to getting this as right as you possibly can. We are saying if you have got those kinds of identifiers whether it is a password, a user alias, an IP address, or something that it will be covered if it falls under two different categories. One would be if it relates to a specific individual or then if whether it is created to maintain a preference profile. That may not cover every way that this information could potentially impact an individual at some time, but I think that would give business enough certainty to understand what is being covered and would cover the great bulk of the situations where people are concerned right now.

Mr. ZANEIS. I think the definition and some—we are in some ways putting the cart before the horse. The choice options that we identify really also matter because when you put a blanket opt-in for third party data usage which is the Internet—we did a survey earlier this year that demonstrated then over 80 percent of all online advertising campaigns used behavioral targeting or techniques. So when you are talking about opt-in for third party data usage, you are talking about the vast majority of the economic engine of the Internet. So it really matters what choice mechanism you give because the stakes really get high. Now in our self-regulatory system that we put out we actually followed very closely the FTC's own definition which was extremely broad and included, you know, sort of all data used for behavioral advertising—online behavioral advertising. But because we had an opt-out requirement instead of an opt-in, it was something that our industry at least—I can speak for us, we could live with that. We could live with the broader definition if we got the choice mechanism right. So I think they all kind of, you know—this is a holistic bill and the different provisions really have to work together. You have had great staff work to put this together and we just need to be cognizant of that, and we stand ready to work through those issues with you.

Mr. RUSH. Do you have any additional questions?

Mr. WHITFIELD. I will just make one other comment. We are in a little bit of a debate about adopting a fully opt-in system in the—we have heard some people say whether it would significantly impact e-commerce in a negative way, how many of you feel that it would? An opt-in system would dramatically impact e-commerce? OK, good. So almost everybody up there, except I guess you Mr. Mierzwinski and——

Ms. HARRIS. There is some ambiguity here. Go ahead.

Mr. VLADECK. I think that we have been struggling with this question for a long time, and I am not speaking for the Commission now. I am speaking for staff. I think there is too much fray given to the question of the label of opt-in or opt-out. The concepts are not self-defining and skilled marketers, and there are lots of them out there, can easily make either method of expressing choice either easy or difficult. We have both given what is called affirmative consent because we have clicked the button and we both, you know, all of us have easily given in to either method. In our view the questions merely doesn't boil down to this label. It is a legal label. It is not really a practical label. We believe that the goal ought to be to insure the consumers are well informed, and are given easy, and clear tools with which to exercise choice. Clarity and ease of use ought to be the key metrics, not easily manipulable legal terms like opt-in, and opt-out. And that is what we think the real problem is.

Mr. WHITFIELD. Thank you, thank you.

Ms. HARRIS. I have nothing to add to that.

Mr. WHITFIELD. We should have asked him a question earlier.

Mr. VLADECK. I am fine.

Mr. RUSH. Well, the Chair—that concludes our questioning. And I merely want to reiterate to the witnesses how appreciative we are for you taking your time to come and share with us your expertise and your insights into this process and into both of the drafts, Mr. Boucher's draft bill and to H.R. 5777. And the Chair wants to assure everyone who is present, including our witnesses, that there will be ample opportunity for more input before we mark up this bill. I am cognizant of the fact that this bill was introduced four days ago and we are having a hearing, but I am also determined that we need to move forward, you know. I am not sure, there won't be—there will be a lot of deliberation, but it won't be unnecessary delay in terms of getting this bill to the floor as it be, and hopefully to the floor. And we want to—what was some—I want to give you assurances that your time is not just being wasted here. It is really—your investment in this process will result in a better bill but it will be a bill that hopefully will become law. And I want to thank you so very much for being here this afternoon. And with that said this Subcommittee is now adjourned.

[Whereupon, at 4:42 p.m., the Subcommittee was adjourned.]

○