COMBATING SPYWARE: H.R. 964, THE SPY ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

ON

H.R. 964

MARCH 15, 2007

Serial No. 110–21

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

39–810 PDF WASHINGTON : 2008

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

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
J. DENNIS HASTERT, Illinois
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
BUD ALBRIGHT, *Minority Staff Director*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BOBBY L. RUSH, Illinois, *Chairman*

JAN SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
BARON P. HILL, Indiana
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
CHARLES A. GONZALEZ, Texas
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
CHARLIE MELANCON, Louisiana
JOHN D. DINGELL, Michigan

CLIFF STEARNS, Florida,
Ranking Member
J. DENNIS HASTERT, Illinois
ED WHITFIELD, Kentucky
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
SUE WILKINS MYRICK, North Carolina
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas

CONTENTS

	Page
H.R. 964, to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.	3
Barton, Hon. Joe, a Representative in Congress from the State of Texas, opening statement	36
Bono, Hon. Mary, a Representative in Congress from the State of California, opening statement	39
Hooley, Hon. Darlene, a Representative in Congress from the State of Oregon, opening statement	37
Rush, Hon. Bobby L., a Representative in Congress from the State of Illinois, opening statement	1
Schakowsky, Hon. Jan, a Representative in Congress from the State of Illinois, opening statement	35
Stearns, Hon. Cliff, a Representative in Congress from the State of Florida, opening statement	34
Towns, Hon. Edolphus, a Representative in Congress from the State of New York, opening statement	38

WITNESSES

Cerasale, Jerry, senior vice president, government affairs, Direct Marketing Association, Inc.	74
Prepared statement	76
Maier, Fran, executive director, TRUSTe	95
Prepared statement	97
Morgan, Dave, founder and chairman, Tacoda, Inc.	87
Prepared statement	89
Schwartz, Ari, deputy director, Center for Democracy and Technology	40
Prepared statement	42
Varney, Christine A., Hogan & Hartson LLP, on behalf of Zango, Inc.	131
Prepared statement	134

COMBATING SPYWARE: H.R. 964, THE SPY ACT

THURSDAY, MARCH 15, 2007

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

The subcommittee met, pursuant to call, at 11:10 a.m., in room 2322 of the Rayburn House Office Building, Hon. Bobby L. Rush (chairman of the subcommittee) presiding.

Members present: Representatives Schakowsky, Barrow, Towns, Ross, Hooley, Matheson, Stearns, Bono, Terry and Barton [ex officio].

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

Mr. RUSH. The subcommittee will come to order.

Today the Subcommittee on Commerce, Trade and Consumer Protection tackles the problem of spyware, the insidious software that consumers unwittingly download onto their computers only to have their personal private information extracted for commercial or fraudulent purposes.

Spyware comes in many forms. Sometimes it takes the form of adware that tracks the Web sites an individual visits in order to facilitate target marketing and develop pop-up ads tailored to sites he or she visits. At other times it is far more offensive, redirecting his or her Web searches to gambling or pornographic sites. And sometimes at its very worst, spyware monitors and steals a consumer's sensitive secret information such as account passwords and credit card numbers. Spyware surreptitiously makes its way onto one's computer by fooling the computer into downloading the nefarious software. Spyware is often secretly bundled with free software from Web sites that a consumer willingly downloads onto his or her computer. At other times spyware is installed as an add-on to a browser's toolbar or it simply pops up as a seemingly innocuous Web site or window, innocently asking for permission to install. Perhaps the worst of all, some spyware masquerades as anti-spyware with promises of cleaning up a person's computer only to install its own version of spyware.

Whatever its form and however it is installed, at its worst spyware can lead to the unwanted exposure of offensive Web content to unsuspecting individuals, particularly children. It can also lead to outright fraud resulting in significant financial damages. At its best, spyware is simply nasty stuff that clogs computers, slows

down processing power and is costly to remove. According to a survey in Consumer Reports as cited in the Washington Post, consumers paid as much as $7.8 billion over 2 years to protect or repair their computers with anti-spyware and anti-virus software.

In the past two Congresses, Mrs. Bono and Mr. Towns introduced the bipartisan Spy Act and both times the bill enjoyed overwhelming support. Twice this subcommittee and the full committee unanimously reported the bill. Twice the full House passed the bill with near unanimity and twice the Spy Act met its demise in the Senate. This year Mr. Towns and Mrs. Bono are once again teaming up to introduce the Spy Act as H.R. 964. It is my full intent as chairman of this subcommittee to do everything I can to make it three times that this bill passes this subcommittee and the full committee and the House of Representatives and finally makes its way to the President's desk. Let us all hope that the Senate can get its act together this time around. Three times should be the charm for the Senate.

H.R. 964 provides a broad regulatory framework that empowers consumers with knowledge and allows them to be in charge of what goes on their personal computers. First, the bill outright prohibits deceptive practices and acts related to spyware that wreak havoc on a computer's operating system or is a harmful invasion of one's privacy. Moreover, the bill creates a regime where an entity cannot execute any program that collects personal information without first giving explicit notice to the consumer and subsequently receiving his or her consent. The bill further requires that once installed, the information collection program can be easily removed or disabled. Lastly, H.R. 964 provides that the FTC will enforce the Spy Act and that any violation of these provisions will be treated as an unfair and deceptive act or practice violating a rule promulgated under section 18 of the FTC Act. Accordingly, the Commission will be able to impose significant penalties, and I firmly believe, as do most of today's witnesses, that this bill strikes an appropriate and workable balance that will allow honest commerce and innovation to occur.

Last year, not only did this bill receive an overwhelming support from our members but also from many technology companies and associations including Yahoo, eBay, AOL Time Warner, Dell, Microsoft, EarthLink and the U.S. Telecom Association. We will carefully consider the testimony of our witnesses and the comment letters that we have received from the FTC, consumer groups and industry experts.

Again, I want to commend Mr. Towns and Mrs. Bono for the terrific work that they have done on the Spy Act and for exhibiting yet another example of quality bipartisan cooperation that is really rather unique to this subcommittee, and I welcome our guests, who have graciously agreed to appear before us today and I hope that today marks the first step towards making this important bill into law.

Thank you.

At this time I will submit a copy of H.R. 964 for inclusion in the record.

[H.R. 964 follows:]

I

110TH CONGRESS
1ST SESSION

H. R. 964

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 8, 2007

Mr. TOWNS (for himself, Mrs. BONO, Mr. DINGELL, Mr. BARTON of Texas, Mr. RUSH, Mr. STEARNS, Mr. MARKEY, Ms. SCHAKOWSKY, Mr. BOUCHER, Mr. GORDON of Tennessee, Ms. ESHOO, Mr. STUPAK, Mr. GENE GREEN of Texas, Ms. DEGETTE, Mrs. CAPPS, Mr. DOYLE, Ms. SOLIS, Mr. GONZALEZ, Mr. INSLEE, Ms. HOOLEY, Mr. WEINER, Mr. MATHESON, Mr. BUTTERFIELD, Mr. HASTERT, Mr. RADANOVICH, Mr. TERRY, Mrs. MYRICK, Mr. BURGESS, and Mr. ENGEL) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, 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.

This Act may be cited as the "Securely Protect Yourself Against Cyber Trespass Act" or the "Spy Act".

SEC. 2. PROHIBITION OF UNFAIR OR DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.

(a) PROHIBITION.—It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in unfair or deceptive acts or practices that involve any of the following conduct with respect to the protected computer:

(1) Taking control of the computer by—

(A) utilizing such computer to send unsolicited information or material from the computer to others;

(B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet—

(i) without authorization of the owner or authorized user of the computer; and

(ii) away from the site the user intended to view, to one or more other Web pages, such that the user is prevented from viewing the content at the intended Web page, unless such diverting is otherwise authorized;

(C) accessing, hijacking, or otherwise using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or au-

1 thorized user or a third party defrauded by
2 such conduct to incur charges or other costs for
3 a service that is not authorized by such owner
4 or authorized user;
5 (D) using the computer as part of an ac-
6 tivity performed by a group of computers that
7 causes damage to another computer; or
8 (E) delivering advertisements that a user
9 of the computer cannot close without undue ef-
10 fort or knowledge by the user or without turn-
11 ing off the computer or closing all sessions of
12 the Internet browser for the computer.
13 (2) Modifying settings related to use of the
14 computer or to the computer's access to or use of
15 the Internet by altering—
16 (A) the Web page that appears when the
17 owner or authorized user launches an Internet
18 browser or similar program used to access and
19 navigate the Internet;
20 (B) the default provider used to access or
21 search the Internet, or other existing Internet
22 connections settings;
23 (C) a list of bookmarks used by the com-
24 puter to access Web pages; or

1 (D) security or other settings of the com-
2 puter that protect information about the owner
3 or authorized user for the purposes of causing
4 damage or harm to the computer or owner or
5 user.
6 (3) Collecting personally identifiable informa-
7 tion through the use of a keystroke logging function.
8 (4) Inducing the owner or authorized user of
9 the computer to disclose personally identifiable infor-
10 mation by means of a Web page that—
11 (A) is substantially similar to a Web page
12 established or provided by another person; and
13 (B) misleads the owner or authorized user
14 that such Web page is provided by such other
15 person.
16 (5) Inducing the owner or authorized user to
17 install a component of computer software onto the
18 computer, or preventing reasonable efforts to block
19 the installation or execution of, or to disable, a com-
20 ponent of computer software by—
21 (A) presenting the owner or authorized
22 user with an option to decline installation of
23 such a component such that, when the option is
24 selected by the owner or authorized user or
25 when the owner or authorized user reasonably

1 attempts to decline the installation, the installa-
2 tion nevertheless proceeds; or
3 (B) causing such a component that the
4 owner or authorized user has properly removed
5 or disabled to automatically reinstall or reac-
6 tivate on the computer.
7 (6) Misrepresenting that installing a separate
8 component of computer software or providing log-in
9 and password information is necessary for security
10 or privacy reasons, or that installing a separate com-
11 ponent of computer software is necessary to open,
12 view, or play a particular type of content.
13 (7) Inducing the owner or authorized user to
14 install or execute computer software by misrepre-
15 senting the identity or authority of the person or en-
16 tity providing the computer software to the owner or
17 user.
18 (8) Inducing the owner or authorized user to
19 provide personally identifiable, password, or account
20 information to another person—
21 (A) by misrepresenting the identity of the
22 person seeking the information; or
23 (B) without the authority of the intended
24 recipient of the information.

1 (9) Removing, disabling, or rendering inoper-
2 ative a security, anti-spyware, or anti-virus tech-
3 nology installed on the computer.
4 (10) Installing or executing on the computer
5 one or more additional components of computer soft-
6 ware with the intent of causing a person to use such
7 components in a way that violates any other provi-
8 sion of this section.
9 (b) GUIDANCE.—The Commission shall issue guid-
10 ance regarding compliance with and violations of this sec-
11 tion. This subsection shall take effect upon the date of
12 the enactment of this Act.
13 (c) EFFECTIVE DATE.—Except as provided in sub-
14 section (b), this section shall take effect upon the expira-
15 tion of the 6-month period that begins on the date of the
16 enactment of this Act.
17 **SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFOR-**
18 **MATION WITHOUT NOTICE AND CONSENT.**
19 (a) OPT-IN REQUIREMENT.—Except as provided in
20 subsection (e), it is unlawful for any person—
21 (1) to transmit to a protected computer, which
22 is not owned by such person and for which such per-
23 son is not an authorized user, any information col-
24 lection program, unless—

1 (A) such information collection program
2 provides notice in accordance with subsection
3 (c) before execution of any of the information
4 collection functions of the program; and
5 (B) such information collection program
6 includes the functions required under sub-
7 section (d); or
8 (2) to execute any information collection pro-
9 gram installed on such a protected computer un-
10 less—
11 (A) before execution of any of the informa-
12 tion collection functions of the program, the
13 owner or an authorized user of the protected
14 computer has consented to such execution pur-
15 suant to notice in accordance with subsection
16 (c); and
17 (B) such information collection program
18 includes the functions required under sub-
19 section (d).
20 (b) INFORMATION COLLECTION PROGRAM.—
21 (1) IN GENERAL.—For purposes of this section,
22 the term "information collection program" means
23 computer software that performs either of the fol-
24 lowing functions:

(A) COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION.—The computer software—

(i) collects personally identifiable information; and

(ii)(I) sends such information to a person other than the owner or authorized user of the computer, or

(II) uses such information to deliver advertising to, or display advertising on, the computer.

(B) COLLECTION OF INFORMATION REGARDING WEB PAGES VISITED TO DELIVER ADVERTISING.—The computer software—

(i) collects information regarding the Web pages accessed using the computer; and

(ii) uses such information to deliver advertising to, or display advertising on, the computer.

(2) EXCEPTION FOR SOFTWARE COLLECTING INFORMATION REGARDING WEB PAGES VISITED WITHIN A PARTICULAR WEB SITE.—Computer software that otherwise would be considered an informa-

1 tion collection program by reason of paragraph
2 (1)(B) shall not be considered such a program if—
3 (A) the only information collected by the
4 software regarding Web pages that are accessed
5 using the computer is information regarding
6 Web pages within a particular Web site;
7 (B) such information collected is not sent
8 to a person other than—
9 (i) the provider of the Web site
10 accessed; or
11 (ii) a party authorized to facilitate the
12 display or functionality of Web pages with-
13 in the Web site accessed; and
14 (C) the only advertising delivered to or dis-
15 played on the computer using such information
16 is advertising on Web pages within that par-
17 ticular Web site.
18 (c) NOTICE AND CONSENT.—
19 (1) IN GENERAL.—Notice in accordance with
20 this subsection with respect to an information collec-
21 tion program is clear and conspicuous notice in plain
22 language, set forth as the Commission shall provide,
23 that meets all of the following requirements:

1 (A) The notice clearly distinguishes such
2 notice from any other information visually pre-
3 sented contemporaneously on the computer.
4 (B) The notice contains one of the fol-
5 lowing statements, as applicable, or a substan-
6 tially similar statement:
7 (i) With respect to an information col-
8 lection program described in subsection
9 (b)(1)(A): "This program will collect and
10 transmit information about you. Do you
11 accept?".
12 (ii) With respect to an information
13 collection program described in subsection
14 (b)(1)(B): "This program will collect infor-
15 mation about Web pages you access and
16 will use that information to display adver-
17 tising on your computer. Do you accept?".
18 (iii) With respect to an information
19 collection program that performs the ac-
20 tions described in both subparagraphs (A)
21 and (B) of subsection (b)(1): "This pro-
22 gram will collect and transmit information
23 about you and will collect information
24 about Web pages you access and use that

1 information to display advertising on your
2 computer. Do you accept?''.
3 (C) The notice provides for the user—
4 (i) to grant or deny consent referred
5 to in subsection (a) by selecting an option
6 to grant or deny such consent; and
7 (ii) to abandon or cancel the trans-
8 mission or execution referred to in sub-
9 section (a) without granting or denying
10 such consent.
11 (D) The notice provides an option for the
12 user to select to display on the computer, before
13 granting or denying consent using the option
14 required under subparagraph (C), a clear de-
15 scription of—
16 (i) the types of information to be col-
17 lected and sent (if any) by the information
18 collection program;
19 (ii) the purpose for which such infor-
20 mation is to be collected and sent; and
21 (iii) in the case of an information col-
22 lection program that first executes any of
23 the information collection functions of the
24 program together with the first execution
25 of other computer software, the identity of

1 any such software that is an information
2 collection program.
3 (E) The notice provides for concurrent dis-
4 play of the information required under subpara-
5 graphs (B) and (C) and the option required
6 under subparagraph (D) until the user—
7 (i) grants or denies consent using the
8 option required under subparagraph (C)(i);
9 (ii) abandons or cancels the trans-
10 mission or execution pursuant to subpara-
11 graph (C)(ii); or
12 (iii) selects the option required under
13 subparagraph (D).
14 (2) SINGLE NOTICE.—The Commission shall
15 provide that, in the case in which multiple informa-
16 tion collection programs are provided to the pro-
17 tected computer together, or as part of a suite of
18 functionally related software, the notice require-
19 ments of paragraphs (1)(A) and (2)(A) of subsection
20 (a) may be met by providing, before execution of any
21 of the information collection functions of the pro-
22 grams, clear and conspicuous notice in plain lan-
23 guage in accordance with paragraph (1) of this sub-
24 section by means of a single notice that applies to
25 all such information collection programs, except that

1 such notice shall provide the option under subpara-
2 graph (D) of paragraph (1) of this subsection with
3 respect to each such information collection program.
4 (3) CHANGE IN INFORMATION COLLECTION.—If
5 an owner or authorized user has granted consent to
6 execution of an information collection program pur-
7 suant to a notice in accordance with this subsection:
8 (A) IN GENERAL.—No subsequent such
9 notice is required, except as provided in sub-
10 paragraph (B).
11 (B) SUBSEQUENT NOTICE.—The person
12 who transmitted the program shall provide an-
13 other notice in accordance with this subsection
14 and obtain consent before such program may be
15 used to collect or send information of a type or
16 for a purpose that is materially different from,
17 and outside the scope of, the type or purpose
18 set forth in the initial or any previous notice.
19 (4) REGULATIONS.—The Commission shall
20 issue regulations to carry out this subsection.
21 (d) REQUIRED FUNCTIONS.—The functions required
22 under this subsection to be included in an information col-
23 lection program that executes any information collection
24 functions with respect to a protected computer are as fol-
25 lows:

1 (1) DISABLING FUNCTION.—With respect to
2 any information collection program, a function of
3 the program that allows a user of the program to re-
4 move the program or disable operation of the pro-
5 gram with respect to such protected computer by a
6 function that—
7 (A) is easily identifiable to a user of the
8 computer; and
9 (B) can be performed without undue effort
10 or knowledge by the user of the protected com-
11 puter.
12 (2) IDENTITY FUNCTION.—
13 (A) IN GENERAL.—With respect only to an
14 information collection program that uses infor-
15 mation collected in the manner described in
16 subparagraph (A)(ii)(II) or (B)(ii) of subsection
17 (b)(1) and subject to subparagraph (B) of this
18 paragraph, a function of the program that pro-
19 vides that each display of an advertisement di-
20 rected or displayed using such information,
21 when the owner or authorized user is accessing
22 a Web page or online location other than of the
23 provider of the computer software, is accom-
24 panied by the name of the information collec-
25 tion program, a logogram or trademark used

1 for the exclusive purpose of identifying the pro-
2 gram, or a statement or other information suffi-
3 cient to clearly identify the program.
4 (B) EXEMPTION FOR EMBEDDED ADVER-
5 TISEMENTS.—The Commission shall, by regula-
6 tion, exempt from the applicability of subpara-
7 graph (A) the embedded display of any adver-
8 tisement on a Web page that contempora-
9 neously displays other information.
10 (3) RULEMAKING.—The Commission may issue
11 regulations to carry out this subsection.
12 (e) LIMITATION ON LIABILITY.—A telecommuni-
13 cations carrier, a provider of information service or inter-
14 active computer service, a cable operator, or a provider
15 of transmission capability shall not be liable under this
16 section to the extent that the carrier, operator, or pro-
17 vider—
18 (1) transmits, routes, hosts, stores, or provides
19 connections for an information collection program
20 through a system or network controlled or operated
21 by or for the carrier, operator, or provider; or
22 (2) provides an information location tool, such
23 as a directory, index, reference, pointer, or hypertext
24 link, through which the owner or user of a protected
25 computer locates an information collection program.

1 **SEC. 4. ENFORCEMENT.**

2 (a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—
3 This Act shall be enforced by the Commission under the
4 Federal Trade Commission Act (15 U.S.C. 41 et seq.).
5 A violation of any provision of this Act or of a regulation
6 issued under this Act shall be treated as an unfair or de-
7 ceptive act or practice violating a rule promulgated under
8 section 18 of the Federal Trade Commission Act (15
9 U.S.C. 57a).

10 (b) PENALTY FOR PATTERN OR PRACTICE VIOLA-
11 TIONS.—

12 (1) IN GENERAL.—Notwithstanding subsection
13 (a) and the Federal Trade Commission Act, in the
14 case of a person who engages in a pattern or prac-
15 tice that violates section 2 or 3, the Commission
16 may, in its discretion, seek a civil penalty for such
17 pattern or practice of violations in an amount, as de-
18 termined by the Commission, of not more than—

19 (A) $3,000,000 for each violation of sec-
20 tion 2; and

21 (B) $1,000,000 for each violation of sec-
22 tion 3.

23 (2) TREATMENT OF SINGLE ACTION OR CON-
24 DUCT.—In applying paragraph (1)—

25 (A) any single action or conduct that vio-
26 lates section 2 or 3 with respect to multiple

1 protected computers shall be treated as a single
2 violation; and
3 (B) any single action or conduct that vio-
4 lates more than one paragraph of section 2(a)
5 shall be considered multiple violations, based on
6 the number of such paragraphs violated.
7 (c) REQUIRED SCIENTER.—Civil penalties sought
8 under this section for any action may not be granted by
9 the Commission or any court unless the Commission or
10 court, respectively, establishes that the action was com-
11 mitted with actual knowledge or knowledge fairly implied
12 on the basis of objective circumstances that such act is
13 unfair or deceptive or violates this Act.
14 (d) FACTORS IN AMOUNT OF PENALTY.—In deter-
15 mining the amount of any penalty pursuant to subsection
16 (a) or (b), the court shall take into account the degree
17 of culpability, any history of prior such conduct, ability
18 to pay, effect on ability to continue to do business, and
19 such other matters as justice may require.
20 (e) EXCLUSIVENESS OF REMEDIES.—The remedies
21 in this section (including remedies available to the Com-
22 mission under the Federal Trade Commission Act) are the
23 exclusive remedies for violations of this Act.
24 (f) EFFECTIVE DATE.—To the extent only that this
25 section applies to violations of section 2(a), this section

1 shall take effect upon the expiration of the 6-month period
2 that begins on the date of the enactment of this Act.

3 **SEC. 5. LIMITATIONS.**

4 (a) LAW ENFORCEMENT AUTHORITY.—Sections 2
5 and 3 shall not apply to—

6 (1) any act taken by a law enforcement agent
7 in the performance of official duties; or

8 (2) the transmission or execution of an infor-
9 mation collection program in compliance with a law
10 enforcement, investigatory, national security, or reg-
11 ulatory agency or department of the United States
12 or any State in response to a request or demand
13 made under authority granted to that agency or de-
14 partment, including a warrant issued under the Fed-
15 eral Rules of Criminal Procedure, an equivalent
16 State warrant, a court order, or other lawful proc-
17 ess.

18 (b) EXCEPTION RELATING TO SECURITY.—Nothing
19 in this Act shall apply to—

20 (1) any monitoring of, or interaction with, a
21 subscriber's Internet or other network connection or
22 service, or a protected computer, by a telecommuni-
23 cations carrier, cable operator, computer hardware
24 or software provider, or provider of information serv-
25 ice or interactive computer service, to the extent that

1 such monitoring or interaction is for network or
2 computer security purposes, diagnostics, technical
3 support, or repair, or for the detection or prevention
4 of fraudulent activities; or
5 (2) a discrete interaction with a protected com-
6 puter by a provider of computer software solely to
7 determine whether the user of the computer is au-
8 thorized to use such software, that occurs upon—
9 (A) initialization of the software; or
10 (B) an affirmative request by the owner or
11 authorized user for an update of, addition to, or
12 technical service for, the software.
13 (c) GOOD SAMARITAN PROTECTION.—No provider of
14 computer software or of interactive computer service may
15 be held liable under this Act on account of any action vol-
16 untarily taken, or service provided, in good faith to remove
17 or disable a program used to violate section 2 or 3 that
18 is installed on a computer of a customer of such provider,
19 if such provider notifies the customer and obtains the con-
20 sent of the customer before undertaking such action or
21 providing such service.
22 (d) LIMITATION ON LIABILITY.—A manufacturer or
23 retailer of computer equipment shall not be liable under
24 this Act to the extent that the manufacturer or retailer
25 is providing third party branded computer software that

1 is installed on the equipment the manufacturer or retailer
2 is manufacturing or selling.

3 **SEC. 6. EFFECT ON OTHER LAWS.**

4 (a) PREEMPTION OF STATE LAW.—

5 (1) PREEMPTION OF SPYWARE LAWS.—This
6 Act supersedes any provision of a statute, regula-
7 tion, or rule of a State or political subdivision of a
8 State that expressly regulates—

9 (A) unfair or deceptive conduct with re-
10 spect to computers similar to that described in
11 section 2(a);

12 (B) the transmission or execution of a
13 computer program similar to that described in
14 section 3; or

15 (C) the use of computer software that dis-
16 plays advertising content based on the Web
17 pages accessed using a computer.

18 (2) ADDITIONAL PREEMPTION.—

19 (A) IN GENERAL.—No person other than
20 the Attorney General of a State may bring a
21 civil action under the law of any State if such
22 action is premised in whole or in part upon the
23 defendant violating any provision of this Act.

24 (B) PROTECTION OF CONSUMER PROTEC-
25 TION LAWS.—This paragraph shall not be con-

1 strued to limit the enforcement of any State
2 consumer protection law by an Attorney Gen-
3 eral of a State.
4 (3) PROTECTION OF CERTAIN STATE LAWS.—
5 This Act shall not be construed to preempt the ap-
6 plicability of—
7 (A) State trespass, contract, or tort law; or
8 (B) other State laws to the extent that
9 those laws relate to acts of fraud.
10 (b) PRESERVATION OF FTC AUTHORITY.—Nothing
11 in this Act may be construed in any way to limit or affect
12 the Commission's authority under any other provision of
13 law, including the authority to issue advisory opinions
14 (under part 1 of volume 16 of the Code of Federal Regula-
15 tions), policy statements, or guidance regarding this Act.
16 **SEC. 7. ANNUAL FTC REPORT.**
17 For the 12-month period that begins upon the effec-
18 tive date under section 12(a) and for each 12-month pe-
19 riod thereafter, the Commission shall submit a report to
20 the Congress that—
21 (1) specifies the number and types of actions
22 taken during such period to enforce section 2(a) and
23 section 3, the disposition of each such action, any
24 penalties levied in connection with such actions, and

1 any penalties collected in connection with such ac-
2 tions; and
3 (2) describes the administrative structure and
4 personnel and other resources committed by the
5 Commission for enforcement of this Act during such
6 period.

7 Each report under this subsection for a 12-month period
8 shall be submitted not later than 90 days after the expira-
9 tion of such period.

10 **SEC. 8. FTC REPORT ON COOKIES.**

11 (a) IN GENERAL.—Not later than the expiration of
12 the 6-month period that begins on the date of the enact-
13 ment of this Act, the Commission shall submit a report
14 to the Congress regarding the use of cookies, including
15 tracking cookies, in the delivery or display of advertising
16 to the owners and users of computers. The report shall
17 examine and describe the methods by which cookies and
18 the Web sites that place them on computers function sepa-
19 rately and together, and shall compare the use of cookies
20 with the use of information collection programs (as such
21 term is defined in section 3) to determine the extent to
22 which such uses are similar or different. The report may
23 include such recommendations as the Commission con-

1 siders necessary and appropriate, including treatment of
2 cookies under this Act or other laws.

3 (b) DEFINITION.—For purposes of this section, the
4 term "tracking cookie" means a cookie or similar text or
5 data file used alone or in conjunction with one or more
6 Web sites to transmit or convey, to a party other than
7 the intended recipient, personally identifiable information
8 of a computer owner or user, information regarding Web
9 pages accessed by the owner or user, or information re-
10 garding advertisements previously delivered to a computer,
11 for the purpose of—

12 (1) delivering or displaying advertising to the
13 owner or user; or

14 (2) assisting the intended recipient to deliver or
15 display advertising to the owner, user, or others.

16 (c) EFFECTIVE DATE.—This section shall take effect
17 on the date of the enactment of this Act.

18 **SEC. 9. FTC REPORT ON INFORMATION COLLECTION PRO-**
19 **GRAMS INSTALLED BEFORE EFFECTIVE**
20 **DATE.**

21 Not later than the expiration of the 6-month period
22 that begins on the date of the enactment of this Act, the
23 Commission shall submit a report to the Congress on the
24 extent to which there are installed on protected computers
25 information collection programs that, but for installation

1 prior to the effective date under section 12(a), would be
2 subject to the requirements of section 3. The report shall
3 include recommendations regarding the means of afford-
4 ing computer users affected by such information collection
5 programs the protections of section 3, including rec-
6 ommendations regarding requiring a one-time notice and
7 consent by the owner or authorized user of a computer
8 to the continued collection of information by such a pro-
9 gram so installed on the computer.

10 **SEC. 10. REGULATIONS.**

11 (a) IN GENERAL.—The Commission shall issue the
12 regulations required by this Act not later than the expira-
13 tion of the 6-month period beginning on the date of the
14 enactment of this Act. In exercising its authority to issue
15 any regulation under this Act, the Commission shall deter-
16 mine that the regulation is consistent with the public in-
17 terest and the purposes of this Act. Any regulations issued
18 pursuant to this Act shall be issued in accordance with
19 section 553 of title 5, United States Code.

20 (b) EFFECTIVE DATE.—This section shall take effect
21 on the date of the enactment of this Act.

22 **SEC. 11. DEFINITIONS.**

23 For purposes of this Act:

24 (1) CABLE OPERATOR.—The term "cable oper-
25 ator" has the meaning given such term in section

1 602 of the Communications Act of 1934 (47 U.S.C.
2 522).
3 (2) COLLECT.—The term "collect", when used
4 with respect to information and for purposes only of
5 section 3(b)(1)(A), does not include obtaining of the
6 information by a party who is intended by the owner
7 or authorized user of a protected computer to receive
8 the information or by a third party authorized by
9 such intended recipient to receive the information,
10 pursuant to the owner or authorized user—
11 (A) transferring the information to such
12 intended recipient using the protected com-
13 puter; or
14 (B) storing the information on the pro-
15 tected computer in a manner so that it is acces-
16 sible by such intended recipient.
17 (3) COMPUTER; PROTECTED COMPUTER.—The
18 terms "computer" and "protected computer" have
19 the meanings given such terms in section 1030(e) of
20 title 18, United States Code.
21 (4) COMPUTER SOFTWARE.—
22 (A) IN GENERAL.—Except as provided in
23 subparagraph (B), the term "computer soft-
24 ware" means a set of statements or instructions
25 that can be installed and executed on a com-

1 puter for the purpose of bringing about a cer-
2 tain result.
3 (B) EXCEPTION.—Such term does not in-
4 clude computer software that is placed on the
5 computer system of a user by an Internet serv-
6 ice provider, interactive computer service, or
7 Internet Web site solely to enable the user sub-
8 sequently to use such provider or service or to
9 access such Web site.
10 (C) RULE OF CONSTRUCTION REGARDING
11 COOKIES.—This paragraph may not be con-
12 strued to include, as computer software—
13 (i) a cookie; or
14 (ii) any other type of text or data file
15 that solely may be read or transferred by
16 a computer.
17 (5) COMMISSION.—The term "Commission"
18 means the Federal Trade Commission.
19 (6) DAMAGE.—The term "damage" has the
20 meaning given such term in section 1030(e) of title
21 18, United States Code.
22 (7) DECEPTIVE ACTS OR PRACTICES.—The
23 term "deceptive acts or practices" has the meaning
24 applicable to such term for purposes of section 5 of
25 the Federal Trade Commission Act (15 U.S.C. 45).

1 (8) DISABLE.—The term "disable" means, with
2 respect to an information collection program, to per-
3 manently prevent such program from executing any
4 of the functions described in section 3(b)(1) that
5 such program is otherwise capable of executing (in-
6 cluding by removing, deleting, or disabling the pro-
7 gram), unless the owner or operator of a protected
8 computer takes a subsequent affirmative action to
9 enable the execution of such functions.
10 (9) INFORMATION COLLECTION FUNCTIONS.—
11 The term "information collection functions" means,
12 with respect to an information collection program,
13 the functions of the program described in subsection
14 (b)(1) of section 3.
15 (10) INFORMATION SERVICE.—The term "infor-
16 mation service" has the meaning given such term in
17 section 3 of the Communications Act of 1934 (47
18 U.S.C. 153).
19 (11) INTERACTIVE COMPUTER SERVICE.—The
20 term "interactive computer service" has the meaning
21 given such term in section 230(f) of the Communica-
22 tions Act of 1934 (47 U.S.C. 230(f)).
23 (12) INTERNET.—The term "Internet" means
24 collectively the myriad of computer and tele-
25 communications facilities, including equipment and

1 operating software, which comprise the inter-
2 connected world-wide network of networks that em-
3 ploy the Transmission Control Protocol/Internet
4 Protocol, or any predecessor or successor protocols
5 to such protocol, to communicate information of all
6 kinds by wire or radio.

7 (13) PERSONALLY IDENTIFIABLE INFORMA-
8 TION.—

9 (A) IN GENERAL.—The term "personally
10 identifiable information" means the following
11 information, to the extent only that such infor-
12 mation allows a living individual to be identified
13 from that information:

14 (i) First and last name of an indi-
15 vidual.

16 (ii) A home or other physical address
17 of an individual, including street name,
18 name of a city or town, and zip code.

19 (iii) An electronic mail address.

20 (iv) A telephone number.

21 (v) A social security number, tax iden-
22 tification number, passport number, driv-
23 er's license number, or any other govern-
24 ment-issued identification number.

25 (vi) A credit card number.

1 (vii) Any access code, password, or ac-
2 count number, other than an access code
3 or password transmitted by an owner or
4 authorized user of a protected computer to
5 the intended recipient to register for, or
6 log onto, a Web page or other Internet
7 service or a network connection or service
8 of a subscriber that is protected by an ac-
9 cess code or password.
10 (viii) Date of birth, birth certificate
11 number, or place of birth of an individual,
12 except in the case of a date of birth trans-
13 mitted or collected for the purpose of com-
14 pliance with the law.
15 (B) RULEMAKING.—The Commission may,
16 by regulation, add to the types of information
17 described in subparagraph (A) that shall be
18 considered personally identifiable information
19 for purposes of this Act, except that such addi-
20 tional types of information shall be considered
21 personally identifiable information only to the
22 extent that such information allows living indi-
23 viduals, particular computers, particular users
24 of computers, or particular email addresses or

1 other locations of computers to be identified
2 from that information.
3 (14) SUITE OF FUNCTIONALLY RELATED SOFT-
4 WARE.—The term suite of "functionally related soft-
5 ware" means a group of computer software pro-
6 grams distributed to an end user by a single pro-
7 vider, which programs are necessary to enable fea-
8 tures or functionalities of an integrated service of-
9 fered by the provider.
10 (15) TELECOMMUNICATIONS CARRIER.—The
11 term "telecommunications carrier" has the meaning
12 given such term in section 3 of the Communications
13 Act of 1934 (47 U.S.C. 153).
14 (16) TRANSMIT.—The term "transmit" means,
15 with respect to an information collection program,
16 transmission by any means.
17 (17) WEB PAGE.—The term "Web page" means
18 a location, with respect to the World Wide Web, that
19 has a single Uniform Resource Locator or another
20 single location with respect to the Internet, as the
21 Federal Trade Commission may prescribe.
22 (18) WEB SITE.—The term "web site" means a
23 collection of Web pages that are presented and made
24 available by means of the World Wide Web as a sin-
25 gle Web site (or a single Web page so presented and

1 made available), which Web pages have any of the
2 following characteristics:
3 (A) A common domain name.
4 (B) Common ownership, management, or
5 registration.

6 **SEC. 12. APPLICABILITY AND SUNSET.**

7 (a) EFFECTIVE DATE.—Except as specifically pro-
8 vided otherwise in this Act, this Act shall take effect upon
9 the expiration of the 12-month period that begins on the
10 date of the enactment of this Act.

11 (b) APPLICABILITY.—Section 3 shall not apply to an
12 information collection program installed on a protected
13 computer before the effective date under subsection (a) of
14 this section.

15 (c) SUNSET.—This Act shall not apply after Decem-
16 ber 31, 2013.

○

Mr. RUSH. I recognize the ranking member of the subcommittee, the gentleman from Florida, Mr. Stearns.

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

Mr. STEARNS. Thank you, Mr. Chairman.

As you have mentioned, we hope that the third time is the charm here. It has been nearly 3 years since the committee first held hearings on the subject of spyware. Although the Internet may seem like it has been around for a long time to many of us, the reality is that it has only been commercially available for a little more than a decade. As rapidly as usage has spread, so too has industry and user practices evolved. We have learned about some of these practices. Obviously spyware is one of those.

Where circumstances warranted, we tried to respond with legislation in this committee, which we did. Some of our efforts of my colleagues resulted in public laws such as Can Spam. Although we like to respond as quickly as possible, we usually try to be as careful as possible to avoid unintended consequences. I don't think we did. I would say, Mr. Chairman, we are on this side ready to move to markup. We think we could move to markup after this hearing because we have had so much support for this bill in the past and we would like to see a markup out of this subcommittee as soon as possible.

Mrs. Bono has showed leadership and Mr. Towns has in the 108th Congress. We have discovered all the bad things about spyware and what it creates. We also learned that most pernicious forms of spyware have more malicious intentions than we realized. Criminals often in other countries have developed programs that can potentially be used to steal a person's identity. A keystroke logger is one example of a program that can capture a consumer's data, which can then be used to commit fraud. Other types of spyware software have been used to hijack a user's computer or to redirect a user's computer to bogus Web sites.

After investigating the damage of potential harm caused by spyware to consumer computers, we passed the bill out of the subcommittee in the 108th. The House likewise passed it, as you have mentioned. Unfortunately, the Senate did not take up the bill and we tried again in the 109th. The committee again unanimously passed the legislation. H.R. 964 is the same bill we unanimously passed in the committee and nearly unanimously in the House last Congress.

There has been, I think, much progress in the industry, I would compliment them, with the adoption of best practices and recognition of the need for consumer consent. We also have seen an increase in the number of enforcement actions. This is all good. That being said, the threat of spyware and the havoc it can inflict on a consumer's computer—or worse, on the identity—remains a real threat. Consumers and businesses are now spending billions of dollars to protect themselves and their computers. To that end, I believe there is still a need for this legislation and so I support H.R. 964. A company that is a bad actor is generally the exception rather than the rule. While criminals may never disappear, legitimate companies are not in business to offend their customers.

I would like to welcome the distinguished panel here. I look forward to their views on H.R. 964.

Mr. Chairman, in closing I would like to thank Mr. Barton for his leadership on this issue during the last two Congresses. I also obviously commend my colleagues, Mrs. Bono and Mr. Towns, and finally I would like to recognize my colleague, the chairman, Mr. Dingell, and Ms. Schakowsky, who was the ranking member when I was the chairman, for her hard efforts in this area too.

With that, Mr. Chairman, I look forward to the hearing.

Mr. RUSH. Thank you.

The committee recognizes the fine gentlewoman from Illinois, Ms. Schakowsky.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Chairman Rush, for holding today's hearing on H.R. 964, the Spy Act.

The proliferation of spyware, covertly installed software that can snatch personal information, has made it necessary that we pass this legislation. And while I am proud to be an original cosponsor of the Spy Act, I hope this is the last time that I say that.

Our committee wanted to be proactive on this issue; we were. I was very proud to work with Mr. Towns and Mrs. Bono and Mr. Stearns and the chairman at the time, Mr. Barton, and Mr. Dingell. We did our work. We got it out of the subcommittee, the committee and the House. And when we first started working on this issue 4 years ago, spyware was not a household word; it is now. People used to be baffled when they found that their Web page settings changed or when their computers became sluggish. They would think that the problem was their computer or the Internet service provider but now the suspect is spyware.

Spyware is a nationwide problem that affects millions of computers from large financial institution servers to home computers. America Online has put occurrences of spyware as high as 80 percent among households with broadband. As broadband becomes more popular in American households, we can only assume spyware will continue to affect our home computers until we give the Federal Trade Commission all the authority it needs to shut down spyware purveyors.

Again, spyware is much more than little annoyances such as slow computers and unwanted popup ads. Those are just symptoms of the real trouble spyware can cause. The spyware is so resourceful that it can snatch personal information from computer hard drives, track every Web site visited and log every keystroke entered. Spyware is a serious threat to consumer privacy and a powerful tool for identity theft, the fastest-growing financial crime. With all the current threats to our country, our homes and our wallets, our computers should not have another worry.

Although we don't want to stop legitimate uses of the software, underlying spyware such as allowing easy access to online newspapers, we do want consumers to have control of their computers and personal information. We have passed this bill with overwhelming bipartisan support in the past two Congresses and I hope this is the Congress that will get the bill signed into law.

So I thank you, Mr. Chairman.

Mr. RUSH. Thank you.

Now the committee will recognize the ranking member of the full committee, Mr. Barton of Texas, for 5 minutes.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Mr. Chairman. I appreciate the courtesy. I was just downstairs in the Energy and Air Quality Subcommittee in one of our hearings on climate change and rushed up here, so I appreciate the courtesy of being allowed to speak as soon as I get here.

Thank you for holding the hearing on the Spy Act and making it a priority. As everyone knows, this is round 3. The committee sent the Spy Act to the floor by unanimous vote in the last Congress and a nearly unanimous vote in the Congress prior to that. The House likewise passed the legislation by a nearly unanimous vote in the last two Congresses. We are here today because the Senate has twice failed in the last Congresses to act on this bill for reasons that are absolutely a mystery to me.

This legislation ought to be an automatic-passage bill. It is a key component to solving the problem of Internet spying, and protecting our constituents from invasions of their privacy. The bill not only receives broad bipartisan support in this institution but many of the big technology players also support the Spy Act: Yahoo, eBay, AOL Time Warner, Dell, Microsoft, EarthLink, the U.S. Telecom Association, just to name a few. We have differences of opinion on the issue of network neutrality, for example, among some of these folks. On this issue, there is 100 percent unanimity.

The reason for the support is evident. Internet spying is more than just an annoyance and more than an invasion of consumers' privacy. It also poses the very real danger of identity theft. Furthermore, spyware often proves dangerous to the consumer's physical property, their personal computers. The scariest part of spyware is that you can have an unwanted, unnoticed program on your computer that captures and reports your keystrokes. What is at stake is a treasure chest of your life's financial secrets, your Social Security number, your bank account number, your credit card number and all kinds of personal passwords. Many consumers don't even know that this is possible, much less that these applications are alive on their computers right now, and as easy as it was to acquire a batch of spyware, sometimes it is almost impossible to get rid of it because of deceptive or nonexistent instructions for uninstalling these applications. You can pick up a batch of spyware by a click of a mouse but you may need the help of a computer expert and all day to get rid of it.

Industry groups have taken strong steps, luckily, towards combating the dangers of spyware. However, it will take a mix of technology, consumer awareness, industry best practices, consumer education, strong enforcement of existing law and I think new law to effectively fight spyware.

The bill before us does that. It places strong enforcement tools in the FTC's toolbox. It provides stiff penalties to hold various ac-

tors accountable for their action. It still balances the interests that are legitimate business interests of the bill.

I could go on and on but let me simply say that this has been a bipartisan effort on our committee. Congresswoman Bono, Congressman Towns, Congressman Stearns, Congresswoman Jan Schakowsky as well as Chairman Dingell and myself have worked diligently to bring this legislation to the floor. And now with your efforts, Mr. Chairman, I am sure that we will finally get it across the finish line and get it through the Senate too. It just takes somebody from Chicago to get it done.

With that, Mr. Chairman, I yield back the balance of my time.

Mr. RUSH. What else do you want?

The gentle lady from Oregon, Ms. Hooley, is recognized for 5 minutes.

OPENING STATEMENT OF HON. DARLENE HOOLEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Ms. HOOLEY. Thank you, Mr. Chairman, and I am thankful to all of the witnesses for being here today and your testimony on this issue.

Although I am new to the Energy and Commerce Committee and this subcommittee, I have been involved for the last 8 years with fraud prevention efforts. I am pleased to join this subcommittee and have the opportunity to address these important issues as they relate to commerce. I commend my colleagues for taking up this issue of spyware, not only this Congress but for the last two Congresses, and I, like the chair and ranking member, hope this legislation can finally get all the way through and become law.

Software that is installed without your consent to monitor or control your computer, known as spyware, threatens the security of our personal information and private transactions. It threatens commerce on the Internet and consumers' confidence of Web purchases and pollutes computers to the point they no longer function. Despite the efforts of FTC, which has completed 11 spyware enforcement cases, and the passage of the Safe Web Act, more needs to be done and I think this legislation is the answer. I do, however, have some concerns with regard to the lack of an exemption for fraud detection software. As I understand it, fraud detection software that is used to make consumers safer and helps protect them from fraudulent activity might be curtailed by this legislation. I hope we can look at this issue before markup.

Again, I applaud this subcommittee for their diligent work on spyware and look forward to working with all of you and passing this piece of legislation.

Thank you, and I yield back.

Mr. RUSH. Thank you.

The gentleman from Nebraska, Mr. Terry, is recognized for 5 minutes.

Mr. TERRY. I pass.

Mr. RUSH. The gentleman from Utah is recognized for 5 minutes.

Mr. MATHESON. I will waive.

Mr. RUSH. The gentleman from New York, the coauthor of the bill, Mr. Towns, is recognized for 5 minutes.

OPENING STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. TOWNS. Thank you very much, Mr. Chairman. I want you to know that I feel very confident and comfortable that this is going to make it all the way with you in the chair and of course seeing Mr. Morgan down from New York and I know that we are going to finish this thing off this time, no doubt about it.

I also want to thank you for holding this important hearing today on H.R. 964, the Spy Act, and for your strong commitment to protecting consumers' privacy on the Internet. As the primary Democratic sponsor, I have been proud to work with Congresswoman Mary Bono. Her tireless efforts on this issue have been unmatched, and I want to thank her for her dedication and commitment to this issue.

We passed this bill out of committee a few times already so perhaps the third time will be a charm. That is why it is important to hold this hearing. We want to make sure to get it right.

Spyware continues to be a nuisance to many of our constituents, even as new and innovative Internet business models have sprung up. There is still some debate about the approach Congress should take to protect consumers from these harmful programs. One computer manufacturer has said that problems related to spyware cause most of their customer complaints. Another company said that spyware accounts for about 50 percent of all tech support calls. Although hard to quantify, this is adding hundreds of millions of dollars in costs for companies.

More importantly, spyware programs can invade consumer privacy by recording and transmitting personal information, monitoring the Web sites you visit or even stealing documents from our computers. Other programs hijack your computer, forcing you to click through multiple screens until you download a program. Finally, all of these programs impair the functionality of a consumer's computer, often slowing its operation to a grinding halt.

Although the problem seems clear, the solution is far from it. Technology changes at a tremendous rate, often making legislation outdated. Additionally, some computer programs which serve legitimate functions such as scanning your system for problems or security breaches or customizing our browser or advertising experience could be classified as spyware if we do not legislate carefully. It seems to me that a key issue is notice. Consumers must get meaningful and accurate notice before they make a decision to download programs that could harm their computers. The FTC should be prosecuting companies that do not provide notice or that provide deceptive notice. Certainly the egregious violators can be prosecuted under existing statutes and the FTC has taken steps in this regard, possibly in reaction to our continued interest in this legislation.

Finally, let me conclude by saluting my colleagues, first Congresswoman Bono for her legislation and leadership on this issue, and of course, let me thank Ranking Member Barton of the full committee and of course former Chairman Stearns and of course former Ranking Member Schakowsky and also Mr. Dingell, who is the chairman of the full committee. I want to thank all of you for

your work and I know that at the end of the day we are going to get this done, so thank you very much, Mr. Chairman.

Mr. RUSH. Thank you. Before we hear the best that we have for today, I want to just bring to the attention of Ms. Hooley, on page 19, line 3, there are provisions here for the detection or prevention of fraudulent activities.

Ms. HOOLEY. OK. What line is it, Mr. Chairman?

Mr. RUSH. Page 19, line 3.

Ms. HOOLEY. Line 3?

Mr. RUSH. Right.

Now I have to personally apologize to the next speaker, a fine member of this subcommittee. Mrs. Bono, I want you to know that we are indeed saving the best for the last, so you are recognized now for 5 minutes.

OPENING STATEMENT OF HON. MARY BONO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mrs. BONO. Thank you, Mr. Chairman, and I just want to mention to my colleague, Mr. Towns, whom I have known for many years, that you reminded me of one of my favorite stories that I ran into Bono in an elevator when I was with my late husband, Sonny Bono, and the two of them had an argument over how to pronounce the name, but Sonny won with "Bono". That is one of my favorite stories and we love to laugh about that.

I want to begin by thanking Chairman Rush and Ranking Member Stearns, again, my colleague, Ed Towns, Ms. Schakowsky and the long list of staff who have worked so hard, especially David Cavicke. They have worked so hard for many years in crafting the Spy Act. I would also like to thank full committee Chairman Dingell and Ranking Member Barton for their leadership and support throughout the past three Congresses. Without their commitment to addressing the problem of spyware, this bill would not be the bipartisan lovefest piece of legislation it is today. In the 108th Congress, I introduced H.R. 2929, the Safeguard Against Privacy Invasions Act. That bill passed the House by a vote of 399 to 1. In the 109th Congress, I reintroduced my spyware bill as H.R. 29, the Securely Protect Yourself Against Spyware Act, or Spy Act, and you don't know how that delights staff to come up with such clever acronyms. But just as it did in the 108th Congress, my bill passed the House by a large margin of 393 to 4.

I remain a strong proponent of spyware legislation because of my belief that our constituents deserve adequate protections when they are online. This means that the computer user should be able to maintain control over his or her computer and the information they store on it. The Spy Act prohibits perverse behavior such as keystroke logging and drive-by downloads. Moreover, it establishes a simple notice regime so that computer users can make informed decisions regarding the programs they wish to put on their computers. Simply stated, this bill works to restore privacy on the personal computer, which has become the control center for our business transactions as well as our personal interactions.

There was a time when the Internet was an occasional tool. However, today the Internet is used by most on a daily basis for practically everything. For this reason, it is crucial that computer users

can securely carry out their lives on the Internet without fear that an unknown party may gain access to sensitive information. It is my firm belief that the Spy Act does this while at the same time preventing negative impacts to legitimate industry and the overall integrity of the Internet.

I look forward to listening to the testimony from our panel today and I am sure that we all agree that spyware is a problem that could undermine the Internet's integrity and needs to be addressed.

I would once again like to thank the committee for its support. I would like to urge my colleagues to support H.R. 964, the Towns-Bono Spy Act.

Again, thank you very much, Mr. Chairman. I yield back my time.

Mr. RUSH. Now we will hear from our fine array of witnesses. We certainly want to thank you for taking your time out from your busy schedule to testify before this subcommittee on this very important matter. I will introduce you individually and we will ask that you restrict your comments, please, to 5 minutes, and then be available for questioning.

Our first witness today is Mr. Ari Schwartz. He is the deputy director of the Center for Democracy and Technology, CDT. CDT is a nonprofit public-interest organization devoted to promoting privacy, civil liberties and democratic values online through legislative, regulatory, self-regulatory and public education efforts. In this capacity, they have been a vocal supporter of comprehensive privacy legislation and further support the goals of H.R. 964, the Spy Act.

Mr. Schwartz, you are recognized for 5 minutes.

STATEMENT OF ARI SCHWARTZ, DEPUTY DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. SCHWARTZ. Chairman Rush, Ranking Member Stearns, members of the committee, thank you for holding this public hearing today on the Spy Act and for inviting me to participate.

This committee has consistently followed the spyware issue over the past 4 years and CDT is pleased to see this much-needed attention continue.

I come back to the committee today to offer good news and bad news on the spyware issue. First the bad news. As predicted by members of this committee in the past, spyware has unquestionably become one of the most serious threats to the Internet's future. Consumer Reports magazine estimates that consumers lost $2.6 billion to spyware alone last year, and one in eight consumers have spyware on their computer and according to the magazine, about 1 million consumers had to throw away their computer because they were so riddled with spyware.

On the other side, in terms of good news, there are new indications that the combination of law enforcement, anti-spyware technology, industry self-regulation, consumer education, legislative efforts and increased responsibility on the part of advertisers are beginning to impact the marketplace that had allowed spyware to flourish.

On the law enforcement front, spyware actions at both the Federal and State level have increased dramatically over the past 2

years. The FTC has now successfully prosecuted 11 cases, which we detailed in our written testimony. Based on the experiences of these cases, it is now clear that the Commission desperately needs increased civil penalty authority in order to be comprehensively effective. The Spy Act, H.R. 964, provides such authority.

Spyware enforcement has also been developing at the State level with 10 cases across four States so far. Although H.R. 964 safeguards State-level enforcement under consumer protection statutes, it does not explicitly preserve the ability for State attorneys general to bring civil actions under statutory provisions specific to spyware. With so much enforcement work now occurring at the State level, we feel it is important to safeguard the role of the State attorney general by empowering them to help enforce Federal law.

On a final note, I would like to stress that the Center for Democracy & Technology still strongly believes that the real long-term solution to spyware and other privacy issues in front of this committee will require baseline consumer privacy legislation based on fair information practices. General privacy legislation would provide businesses with guidance as they deploy new technologies and business models that involve the collection of information and it would give consumers some measure of confidence that their privacy is being protected as companies roll out these new ventures. If we do not begin to address privacy issues more comprehensively, this committee will need to continue to address new emerging privacy threats every few months with new legislation in order to protect consumers in the networked economy.

We have seen a number of issues already begin to increase with the most recent including spam, do-not-call lists, search information, data breaches, use of Social Security numbers, pretexting and spyware. While we appreciate the committee's hard work on all these important issues, we believe that the members of this committee should join with the 13 companies and multiple consumer groups that have actively supported comprehensive consumer privacy legislation in an attempt to address these issues at the source rather than continue a piecemeal approach each time a new privacy threat arises.

Thank you for your attention. I look forward to your questions.

[The prepared statement of Mr. Schwartz follows:]

Testimony of

Ari Schwartz, Deputy Director
Center for Democracy and Technology
before
The House Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
on
"Combating Spyware: H.R. 964, the Spy Act"

March 15, 2007

Chairman Rush and Ranking Member Stearns, thank you for holding this hearing on spyware, which continues to be a major problem for consumers and businesses alike. CDT is honored to have the opportunity to participate in the Committee's hearing on this important topic.

CDT is a non-profit public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet. CDT has been a widely recognized leader in the policy debate about the issues raised by spyware.[1] Since CDT last testified before the Committee about spyware, in January 2005, the Federal Trade Commission has completed 11 spyware enforcement actions, three of which were based at least in part on petitions submitted by CDT. Over the past two years, CDT has also convened the Anti-Spyware Coalition (ASC), a group dedicated to building consensus about definitions and best practices in the debate surrounding spyware. The ASC's work to create uniform language and guidelines that can be used across the software industry has been beneficial for both consumers and software makers.

As an organization dedicated both to protecting consumer privacy and to preserving openness and innovation online, CDT has sought to promote responses to the spyware epidemic that provide meaningful protection for users while avoiding unintended consequences that could harm the open, decentralized Internet. We've worked with this committee now for several years, and during that time we've been consistently impressed with its open, deliberative approach to this complex issue.

---

[1] For example, CDT leads the Anti-Spyware Coalition (ASC), a group of anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware; In 2006, CDT Deputy Director Ari Schwartz won the RSA Award for Excellence in Public Policy for his work in building the ASC and other efforts against spyware. *See also* "Eye Spyware," *The Christian Science Monitor*, Apr. 21, 2004 ["Some computer-focused organizations, like the Center for Democracy and Technology, are working to increase public awareness of spyware and its risks."]; "The Spies in Your Computer," *The New York Times*, Feb. 18, 2004 ["Congress will miss the point (in spyware legislation) if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user."]; John Borland, "Spyware and its discontents," *CNET News.com*, Feb. 12, 2004 ["In the past few months, Ari Schwartz and the Washington, D.C.-based Center for Democracy and Technology have leapt into the front ranks of the Net's spyware-fighters."].

Summary

Although we have seen advances in the fight against spyware, millions of consumers are still losing money, time and peace of mind to this online scourge. CDT believes that the necessary framework for combating spyware involves a combination of law enforcement, anti-spyware technology, industry self-regulation and consumer education, legislation, and increased responsibility on the part of advertisers.

On the law enforcement front, the number of spyware actions at the federal level has increased dramatically since this Committee reported spyware legislation during the 109th Congress. The FTC has had a successful run in pursuing spyware cases, but the Commission needs increased civil penalty authority in order to be comprehensively effective. H.R. 964 provides such authority.

Spyware enforcement has also been developing at the state level, with 10 cases across four states thus far. Although H.R. 964 safeguards state-level enforcement under consumer protection statutes, it does not explicitly preserve the ability for state attorneys general to bring civil actions under statutory provisions specific to spyware. With all of the enforcement work going on at the state level, we feel it is important to safeguard the role of state attorneys general by empowering them to help enforce federal law.

We remain firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline privacy legislation. General privacy legislation would provide businesses with guidance as they deploy new technologies and business models that involve the collection of information. At the same time, a baseline law would give consumers some measure of confidence that their privacy is protected as companies roll out new ventures.

There are now 13 major companies that have joined with consumer groups in support of baseline privacy legislation.[2] If we do not begin to address privacy issues more comprehensively, the same players will be back in front of this Committee in a few months to address the next emerging threat to online privacy. We hope that we can address these issues in a way that obviates the need to enact new legislation each time a new privacy threat arises.

I. Understanding and Combating the Spyware Problem

When CDT last testified before this Committee about spyware, little data existed to quantify the size and impact of the spyware problem. Research conducted over the past two years, however, has produced some alarming results. Consumer Reports estimates that spyware cost consumers $2.6 billion last year and affected 1 in 8 Internet users.[3] An

---

[2] See *Consumer Privacy Legislative Forum Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, June 2006, http://www.cdt.org/privacy/20060620cplstatement.pdf. General Electric announced its support after the statement was issued.
[3] "State of the net 2006," *ConsumerReports.org*, Sept. 2006,

AOL/National Cyber Security Alliance study conducted in 354 homes found that 61% of users had spyware installed on their computers.[4] And the Pew Internet & American Life Project reported that nine out of ten Internet users say they have altered their behavior online due to fear of malicious software.[5] All of these figures indicate that while we have seen advances in the fight against spyware, it continues to be a problem for many consumers.

CDT has long endorsed a multi-faceted approach to the spyware problem. We believe that the appropriate framework incorporates the following components:

- *Anti-spyware technology* – Anti-spyware software is a consumer's first defense against spyware infections. The collaboration fostered amongst technology vendors and public interest groups by the Anti-Spyware Coalition has helped to increase the usefulness of these technologies, which, in turn, creates a safer Internet experience for consumers.

- *Industry self-regulation and consumer education* – Helping industry and consumers understand the threat that spyware poses is an essential component of this framework. CDT has been active in the TRUSTe Trusted Download Program and the StopBadware campaign coordinated by Harvard's Berkman Center. Both of these have helped consumers and companies better understand the spyware issue.

- *Responsible advertising* – Large, well-respected companies help to fund the spread of unwanted and harmful adware by paying for advertisements generated by those unwanted programs. The New York attorney general's recent action against three high-profile advertisers,[6] along with public pressure from the FTC,[7] CDT,[8] and others has begun to increase advertiser awareness and accountability.

---

http://www.consumerreports.org:80/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm.

[4] *AOL/NCSA Online Safety Study*, America Online and the National Cyber Security Alliance, Dec. 2005, http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

[5] Susannah Fox, *Spyware: The threat of unwanted software programs is changing the way people use the internet*, Pew Internet & American Life Project, July 6, 2005, http://www.pewinternet.org/PPF/r/160/report_display.asp.

[6] See *In the Matter of Priceline.com Incorporated* (filed Oct. 23, 2006); *In the Matter of Travelocity.com LP* (filed Dec. 18, 2006); and *In the Matter of Cingular Wireless LLC* (filed Jan. 29, 2007), all available at http://www.oag.state.ny.us/press/2007/jan/adware-scannedAODs.pdf.

[7] See, e.g., Cindy Skrzycki, "Stopping Spyware at the Source," *The Washington Post*, Mar. 6, 2007 ["'We need to stop the demand side of spyware,' said Jon Leibowitz, one of the five [FTC] commission members and a Democrat. 'We will send letters to major corporations and entities that place the majority of these ads. This is a wake-up call to put them on notice. That would be a good way to choke off the money.'"].

[8] See *Following the Money: How Advertising Dollars Encourage Nuisance or Harmful Adware and What Can be Done to Reverse the Trend*, Center for Democracy & Technology, May 2, 2006, http://www.cdt.org/privacy/20060320adware.pdf; and *Following the Money II: The Role of Intermediaries in Adware Advertising*, Center for Democracy & Technology, Aug. 2006, http://www.cdt.org/privacy/20060809adware.pdf.

- *Law enforcement* – The enforcement landscape has seen many changes over the past two years. The implications of these changes are discussed in section II below.

- *Legislation* – Legislative approaches to fighting spyware at the federal level fall into two broad categories – attempts to narrowly address the issues raised by spyware, and attempts to deal with the underlying privacy issues in a coherent, long-term fashion. H.R. 964, which we address in sections II and III below, is an example of the first approach. CDT has appreciated the opportunity to work with the Committee on this bill and is generally supportive of this effort, particularly because of the increased civil penalty authority it grants to the FTC for use in prosecuting spyware cases. At the same time, we remain firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline privacy legislation, as discussed in section IV below.

II. Spyware Enforcement and H.R. 964

The spyware enforcement landscape looks vastly different than it did two years ago when CDT last expressed concern to the Committee about the lack of enforcement activity. When the Spy Act passed out of the House in 2005, the FTC had issued complaints against two spyware distributors and one state attorney general had sued one spyware company. As of this writing, the FTC has completed 11 spyware enforcement cases and four states have conducted a total of 10 spyware lawsuits.[9] The following sections explain the implications of FTC and state spyware enforcement for H.R. 964.

FTC Spyware Enforcement

The FTC filed the nation's first spyware lawsuit in 2004 against a network of deceptive adware distributors and their affiliates.[10] The scammers involved were secretly installing software that left consumers' computers vulnerable to hackers, and then duping those same users into purchasing fake security software to help repair their systems. Not only did the FTC succeed in the case – obtaining a $4 million order against the primary defendant and over $300,000 in disgorgement from the other defendants – but the investigations in the case opened up several additional leads that contributed to the FTC's pursuit of other malicious software distributors. In the more than two years since launching this first suit, the FTC has used its broad authority under Title 5 of the FTC Act to pursue cases that cover a wide range of malicious software behaviors, all of which have ended with settlements or court orders that benefit consumers.

The FTC's enforcement efforts have also played an integral role in establishing standards for the software industry as a whole. In two of its most recent enforcement efforts, the FTC reached settlement agreements with major adware distributors Zango Inc. and

[9] See Appendix A for a summary of all FTC, state, and Department of Justice spyware enforcement actions.
[10] *FTC v. Seismic Entertainment, Inc., et al.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

DirectRevenue LLC that required the distributors to clearly and conspicuously disclose material terms about their adware programs *outside of any End User License Agreement (EULA).*[11] With these requirements the FTC has set a disclosure guideline that can be applied across the software industry, for the benefit of consumers. Not only were the adware distributors themselves forced to abandon the practice of offering deceptive or nonexistent disclosures, but software vendors throughout the industry were also put on notice about what constitutes legitimate behavior. The FTC's leadership in this respect has helped to curb uncertainty in the software industry while creating a better online experience for consumers.

While these settlements set important precedents, the monetary relief obtained by the Commission was not commensurate with the harms perpetrated on consumers. Zango, a company that used deceptive tactics to earn over $50 million in revenue in 2004 alone,[12] settled for a mere $3 million with the FTC.[13] The founders of DirectRevenue have pocketed a combined $23 million,[14] yet the FTC's proposed settlement requires only a $1.5 million payment.[15] As FTC Commissioner Jon Leibowitz noted in his dissenting statement in the DirectRevenue case, these numbers are disappointing because they leave the owners of the adware companies "lining their pockets . . . from a business model based on deceit."[16]

The increased civil penalty authority granted by H.R. 964 provides the FTC with the means to obtain more appropriate monetary relief. By giving the FTC explicit authority to seek large civil penalties for spyware infractions, the Commission will be much less encumbered and much more willing to obtain monetary relief commensurate with the harms committed. Both CDT and officials at the FTC have long been supportive of increased penalties, and we are pleased to see them included in H.R. 964.

State Spyware Enforcement

Several state attorneys general have become active in challenging spyware purveyors under state consumer protection, trespass, business practices, and spyware laws. In some of these cases the state attorneys general have taken the lead in nabbing high-profile offenders. For example, Texas took swift action against Sony BMG after it was discovered that the company had distributed millions of audio CDs containing spyware, and New York launched the nation's first investigation into DirectRevenue, nearly a year

---

[11] *See In the Matter of Zango, Inc., formerly known as 180solutions, Inc., Keith Smith, and Daniel Todd*, FTC File No. 052 3130 (filed Nov. 3, 2006), available at http://www.ftc.gov/os/caselist/0523130/index.htm; *In the Matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook*, FTC File No. 052 3131 (filed Feb. 16, 2007), available at http://ftc.gov/os/caselist/0523131/index.htm.

[12] "Inc. Magazine Reveals America's 500 Fastest Growing Private Companies," Zango Inc., Nov. 1, 2005, http://www.zango.com/Destination/Corporate/ReadArticle.aspx?id=36.

[13] See *supra* note 11.

[14] Ben Elgin and Brian Grow, "The Plot to Hijack Your Computer," *BusinessWeek*, July 17, 2006, http://www.businessweek.com/magazine/content/06_29/b3993001.htm.

[15] See *supra* note 11.

[16] *Dissenting Statement of Commissioner Jon Leibowitz In Re DirectRevenue LLC, et al., File No. 052 3131*, Feb. 16, 2007, http://www.ftc.gov/os/caselist/0523131/0523131directrevenueleibowitzstmnt.pdf.

before the FTC announced its settlement with the company. That litigation is still pending.

This growth in spyware enforcement at the state level in particular has several implications for H.R. 964. All of the state spyware cases have invoked state consumer protection laws, and thus we are pleased that Section 6(a)(2)(B) safeguards the authority of state attorneys general to challenge spyware practices under consumer protection statutes. What H.R. 964 does not safeguard, however, is the ability for state attorneys general to bring civil actions under statutory provisions specific to spyware. H.R. 964 preempts state spyware statutes without giving state attorneys general explicit authority to bring civil actions under the new federal law.

Six out of the 10 state spyware cases have invoked state spyware laws. If these state-level laws were to be replaced with a single federal standard, we feel it would be important to preserve the role of state attorneys general by empowering them to help enforce federal law. We understand that adding authority for state attorneys general raises jurisdictional issues, but we feel that this vital component of spyware enforcement must be addressed.

III. Comments on Specific H.R. 964 Language

CDT has minor suggestions on two specific parts of the bill.

First, CDT believes that Section 4(b) of H.R. 964, which gives the FTC explicit authority to seek civil penalties for pattern or practice violations of the Spy Act, will effectively increase the deterrent effect of spyware enforcement. However, it is important for the statute to be clear about what constitutes a "single action or conduct" in violation of the Act, because each single action or conduct carries either the $3 million or $1 million penalty as described in Section 4(b)(1). For example, DirectRevenue is a company that distributed similar software under a handful of different names and through dozens of different distribution channels and schemes. Had the FTC been able to bring its case against DirectRevenue under the Spy Act, we would hope that each of the different software distributions would be considered a "single action or conduct," and thus the civil penalty sought by the FTC could be commensurate with the harm caused. We believe this clarification – that software provided by a single entity using multiple versions, configurations, or distributions can cause multiple violations – may be appropriately addressed in the Committee Report for H.R. 964.

Second, the definition of "personally identifiable information" provided in Section 11(13)(A) includes a list of different types of information that may be used to identify a living individual. An email address is one piece of information in this list, but in some cases email addresses cannot be used to determine the "real world" identity of particular individuals. Thus, some interpretations of this language could exempt email addresses from the definition of personally identifiable information. We believe that this would be a mistake, and we suggest that in Section 11(13)(A) the phrase "allows a living individual to be identified" should be replaced with "allows a living individual to be identified *or contacted*." This will ensure that email addresses are considered as part of PII, since a

person can generally be contacted via email even if the email address does not identify the person.

IV. General Privacy Legislation and H.R. 964

Since our first testimony on this issue, we have urged the Committee to consider how some provisions of the Spy Act may be better addressed in baseline consumer privacy legislation. In light of the growing momentum behind this effort and the numerous other consumer and government privacy issues facing this Congress, we hope that the Committee will revisit these issues. For example, Section 3(c)(1)(B) of H.R. 964 prescribes specific notice language for software. Given the influence that H.R. 964 may have on the broader privacy debate, we have misgivings about a notice approach that specifies disclosure language in statute. Addressing notice at this level of detail in this bill could risk conflicting with or establishing difficult precedents for more general notice provisions in a broader privacy law.

A comprehensive privacy law may also address behaviors that have been omitted by the specificity of H.R. 964. For example, Section 3(b)(1)(B) includes in the definition of "information collection program" computer software that collects information about Web pages accessed on the computer and uses such information to display advertising on the computer. The statute does not, however, cover computer software which is used to collect information about Web pages accessed where that information is later disclosed to a third party but not directly used for advertising purposes. A broader privacy bill could help plug such gaps in H.R. 964.

V. Conclusion

CDT would like to thank the Committee for its hard work and openness throughout the spyware legislation process. While we believe H.R. 964 provides valuable increases to FTC civil penalty authority, we have several concerns with the bill. These include the bill's pre-emption of state-level enforcement in an area where states are proving effective and interstate commerce has not been negatively affected, and the bill's potential impact on the process of crafting and implementing general privacy legislation. We look forward to continuing to work with the Committee in addressing these issues and developing the strongest possible framework to protect consumer privacy in the digital age.

Appendix A: Summary of FTC, State, and Department of Justice Spyware Enforcement Actions

FTC Spyware Case Summary

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
FTC v. Seismic Entertainment Productions, Inc., SmartBot.Net, Inc., and Sanford Wallace Additional defendants: Jared Lansky, John Robert Martinson, OptinTrade, Inc., Mailwiper, Inc., Spy Deleter, Inc. Docket #042-3142	• Installing software onto users' computers that makes substantial modifications to the Internet Explorer Web browser (including the home page and default search engine) without users' knowledge or authorization. • Installing software onto users' computers that in turn creates security holes through which more advertising software and other software is downloaded, all without users' knowledge or authorization. • Inducing users to purchase anti-spyware software products that purport to fix computer problems that the anti-spyware product company itself caused by previously installing software on users' computers without their knowledge or authorization.	Default judgment issued against Wallace and SmartBot.Net:[17] • Ordered to give up over $4 million in ill-gotten gains. • Barred from downloading spyware onto consumers' computers; from downloading any software without consumers' consent; from redirecting consumers' computers to sites other than those the consumers selected to visit; from changing any Web browser's default home page; and from modifying or replacing the search features of any search engine. Settlement reached with Lansky and OptinTrade: • Ordered to give up $227,000 in ill-gotten gains. • Barred from the same practices as Wallace and Smartbot.Net. Seismic Entertainment filed for bankruptcy. Settlement reached with John Robert Martinson and Mailwiper: • Ordered to give up $40,000 in ill-gotten

[17] For the settlements listed in the "Status" column of all three charts in this Appendix, defendants admitted no wrongdoing unless otherwise noted.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		gains with a suspended judgment of $1.86 million. • Barred from the same practices as Wallace and Smartbot.Net http://www.ftc.gov/os/caselist/0423142/0423142.htm
FTC v. MaxTheater, Inc., and Thomas L. Delanoy Docket #042-3213	• Expressly representing or implying that local or remote scans or other examinations of users' computers for spyware had been performed and that spyware had been detected when no such scans or examinations took place and no spyware was detected. • Expressly representing or implying that an anti-spyware product removes all or substantially all spyware on a user's computer when it does not do so.	Settlement reached ordering defendants to give up $76,000 in ill-gotten gains (the full amount of consumer injury). Defendants barred from selling or marketing any anti-spyware product or service in the future; from downloading or installing spyware on consumers' computers, or from assisting others in downloading or installing it; and from making marketing misrepresentations. http://www.ftc.gov/os/caselist/0523059/0523059.htm
FTC v. TrustSoft, Inc. d/b/a Swanksoft and SpyKiller, and Danilo Ladendorf Docket #052-3059	• Expressly representing or implying that remote scans or other examinations of users' computers for spyware had been performed and that spyware had been detected when no such scans or examinations took place and no spyware was detected. • Expressly representing or implying that certain software on a user's computer is spyware (when it is not) after the user downloads and activates an anti-spyware product. • Expressly representing or implying that a spyware removal product removes all, substantially all, or all traces of spyware on a user's computer when it does not do so.	Settlement reached ordering defendants to give up $1.9 million in ill-gotten gains. Settlement bars defendants from making deceptive claims in the sale, marketing, advertising, or promotion of any goods or services and prohibits them from making the specific misrepresentations used in promoting SpyKiller. Defendants barred from using the spyware their "anti-spyware" software supposedly detects and destroys to deliver ads. http://www.ftc.gov/os/caselist/0523059/0523059.htm

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
In the matter of Advertising.com, Inc. a/d/b/a Teknosurf.com, and John Ferber Docket #042-3196	• Disclosing only within a EULA that software to be downloaded by a user includes adware that collects information about the user (including URLs of visited pages and the user's IP address) and serves a substantial number of pop-up ads to the user.	Final consent order issued prohibiting respondents from making any representations about the performance, benefits, efficacy, or features of its programs promoted as security or privacy software, unless they clearly and conspicuously disclose that consumers who install the program will receive advertisements, if that is the case. http://www.ftc.gov/os/caselist/0423196/0423196.htm
FTC v. Odysseus Marketing, Inc, and Walter Rines Docket #042-3205	• Disclosing only within a EULA that software to be downloaded by a user will also cause the installation of additional software that may replace search engine results, collect and transmit information to third parties, deliver pop-up ads, and download more software. • Failing to provide an effective means for users to locate and remove software after it has been downloaded.	Settlement reached ordering defendants to give up $10,000 in ill-gotten gains, with a suspended judgment of $1.75 million. Defendants are also prohibited from producing or distributing software that exploits a security vulnerability, installs without user consent, is overly difficult to uninstall, changes browser settings such as home page, or alters the System32 folder in the Windows operating system. Defendants are further prohibited from gathering personally identifiable information without consumer's consent, selling, or using such information. Finally, defendants are prohibited from making any representation as to the efficacy or performance of software. http://ftc.gov/os/caselist/0423205/0423205.htm

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
FTC v. Enternet Media, Inc., Conspy & Co., Inc., Lida Rohbani, Nima Hakimi, Baback (Babak) Hakimi, and Nicholas C. Albert Docket #052-3135	• Expressly representing or implying that software functions as an innocuous free program or file (including as a browser upgrade or other security software, or as a music file, song lyric, or ring tone) when the software instead causes a stream of ads to appear on users' computers and/or tracks users' Internet activity. • Providing software that does the following when it is installed[18]: (1) tracks users' Internet activity, (2) changes users' Internet homepage settings, (3) inserts a toolbar onto users' Internet browsers, (4) inserts a large side advertising frame or window onto users' browsers, and (5) displays numerous pop-up ads even when users' browsers are closed. • Furnishing others, including affiliate marketers, with software that substantially interferes with consumers' use of their computers and with marketing media that contains false representations regarding that software. • Failing to disclose that music files users can download and incorporate on their own Web sites contain additional code that delivers ads to users' computers. • Failing to disclose that music files downloaded and incorporated on users' Web sites will display ads that prompt site visitors to download other software represented as browser upgrades or other security software.	Settlement reached with Defendant Albert ordering him to give up $3,300 in ill-gotten gains. Defendant is enjoined from distributing software that interferes with consumers' computer use and from making false or misleading representations. Defendant is required to do substantial due diligence if he is to participate in any affiliate program. Settlement reached ordering remaining defendants to give up $2.045 million in ill-gotten gains, with a suspended judgment of $8.5 million. Defendants are also enjoined from making false or misleading representations about the nature, performance, features or cost of software code, publishing software that interferes with a consumer's computer use, or helping others to do so. http://www.ftc.gov/os/caselist/0523135/0523135.htm

[18] In CDT's reading of the FTC complaint against Enternet Media, this set of behaviors *on its own* does not constitute an unfair practice. Rather, the unfair practice was marketing the software without telling consumers it behaved in all those ways and without giving consumers choice about them.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status

FTC
v.
Digital Enterprises, Inc, d/b/a Movieland.com; Triumphant Videos, Inc., d/b/a Popcorn.net; Pacificon International, Inc., d/b/a Vitalix; Alchemy Communications, Inc.; AccessMedia Networks, Inc.; Film Web, Inc.; Binary Source, Inc., d/b/a Moviepass.tv; Medicaster, Inc., d/b/a Medicaster.net; CS Hotline, Inc.; Easton Herd; and Andrew Garroni
 	
Docket #062-3008
	• Expressly representing or implying that the computer owner or user knowingly consented to the installation of software that would repeatedly launch lengthy pop-up payment demands, when neither the owner nor any user consented to the installation.
	• Expressly representing or implying that the computer owner is responsible to satisfy any contract that any other person entered into while using the computer, when this is not the case.
	• Causing software to be installed on consumers' computers that repeatedly launches textual and audiovisual pop-up payment windows that:
	  o remain open for 40 seconds and cannot be closed or minimized through reasonable means,
	  o reappear more and more often as time passes, and
	  o demand that consumers pay at least $29.95 to stop the pop-ups from happening.
	• Causing software to be installed on consumers' computers such that it cannot be located or removed through the use of reasonable efforts.
	• Causing software to be installed on consumers' computers that makes changes to consumers' computers that actively prevent consumers from using the Windows Control Panel to uninstall the software.
	
	-12-
		Stipulated interim agreements reached.
		Defendants are:
		• Prohibited from making representations that computer owners or users are required to pay for software when that is not the case.
		• Required to clearly and prominently disclose the nature, frequency, and duration of pop-up payment windows prior to obtaining consent from computer owners or users to download software that will cause the pop-ups.
		• Required to obtain consent from computer owners or users prior to installing software.
		• Prohibited from displaying pop-up windows more than five times in one day.
		• Prohibited from displaying pop-up ads that cannot easily be closed or whose audio is not easily silenced.
		• Prohibited from displaying pop-up ads that only appear when all other windows are closed.
		
		Defendants Alchemy Communications, Inc. and AccessMedia Network, Inc. are additionally required to provide clear and prominent links on their pop-ups and home pages to a customer service Web site with a toll-free customer service telephone number and email utility. Other defendants are prohibited from interfering with the efforts of Alchemy Communications, Inc. and AccessMedia Networks, Inc. in complying with their stipulated interim agreement.
		
		http://www.ftc.gov/os/caselist/0623008/index.htm

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
In the Matter of Zango, Inc., f/k/a 180solutions, Inc., Keith Smith and Daniel Todd Docket #052-3130	• Using third-party affiliates and sub-affiliates to bundle and install advertising software with other programs without adequately disclosing the existence of the advertising software. • Installing advertising software programs, through affiliates and sub-affiliates, without consumers' knowledge or authorization. • Failing to provide a means for consumers to identify, locate, and remove advertising software.	Settlement reached, ordering respondents to pay $3 million to the FTC. Respondents are forbidden from: • Displaying advertisements to any customer who obtained advertising software prior to January 1, 2006. • Exploiting security vulnerabilities in Internet browsers to install software. • Installing software without obtaining express consent from users. Respondents are obligated to: • Establish and publicize a consumer complaint mechanism that allows consumers to receive timely responses to their complaints about the advertising software. • Maintain a program to ensure that affiliates obtain proper consent from consumers before installing software. • Identify the software program that causes advertisements to be shown to consumers on the advertisements themselves. • Provide links to the consumer complaint mechanism on the advertisements themselves. • Provide consumers with a reasonable means of uninstalling the advertising software.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		http://www.ftc.gov/os/caselist/0523130/index.htm
FTC v. ERG Ventures, LLC and d/b/a ERG Ventures, LLC2, Media Motor, Joysticksavers.com, and PrivateinPublic.com; Elliot S. Cameron; Robert A. Davidson, II; Gary E. Hill; Timothy P. Taylor Docket #062-3192	• Representing that software operates as a standalone innocuous free program, such as a screensaver or icon, when that is not the case. • Failing to disclose that software or content being offered contains additional code and files that cause advertisements, track Internet usage and alter browser settings and existing software products. • Proceeding with installation of software packages despite the fact that a user has declined the terms of the software's End User License Agreement. • Installing software on users' computers that changes browser home pages, adds a menu bar to Internet browsers, tracks consumer's Internet usage, generates pop-ups (occasionally pornographic), degrades computer performance and attacks and degrades anti-spyware software.	Temporary injunction issued. Defendants ordered to halt installation of software that fails to disclose its own name and function and fails to offer a means to users to prevent the installation of such software. Defendants are also prohibited from making and distributing software that: • Tracks consumers' Internet activity. • Changes browser settings, including security settings or home pages. • Generates numerous pop-up advertisements, even while browsers are closed. • Tampers with, disables or otherwise alters the performance of other programs, including anti-spyware or anti-virus programs. Defendants' assets are also frozen. http://www.ftc.gov/os/caselist/0623192/index.htm
In the matter of Sony BMG Music Entertainment, a general partnership Docket # 062-3019	• Failing to adequately disclose that audio CDs will install software on consumers' computers that limits the number of possible copies and file formats of the audio files. • Failing to adequately disclose that the bundled media player on an audio CD will transmit the consumer's Internet Protocol (IP) address and an album identifier to remote Internet servers for the purposes of displaying images and promotional messages on the consumer's	Proposed settlement reached. Defendant is required to: • Clearly and prominently disclose on product packaging that: o software to limit the number of copies and file formats of audio files will be installed on consumers' computers, and

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	computer. • Causing content protection software which may expose consumers' computers to security risks to be installed on consumers' computers without adequate notification and consent. • Failing to provide a way for consumers to locate and/or remove content protection software through reasonable efforts, and thereby causing consumers to incur substantial costs.	○ consumers who decline to install content protection software from an audio CD will not be able to listen to the CD on a computer. • Obtain consent from consumers prior to installing software. • Destroy information collected about consumers through the use of audio CDs within three days of its receipt. • Clearly and prominently disclose on consumers' computer screens that: ○ information about consumers, their computers, or their use of audio CDs will be transmitted over the Internet, and ○ consumers who decline to permit transmission of information about them, their computers, or their use of their audio CDs will not be able to listen to the CDs on a computer. • Obtain consent from consumers prior to transmitting information about them, their computers, or their use of audio CDs. • Continue to provide consumer redress and assistance by posting information on the Web, buying advertising to explain the content protection software's security vulnerability, offering software patches, and compensating consumers monetarily and with additional audio CDs or music

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		downloads. Defendant is prohibited from: • Using information collected about consumers through the use of audio CDs for any marketing purposes. • Installing software that cannot be readily located and removed by a consumer. http://www.ftc.gov/os/caselist/0623019/index.htm
In the matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook Docket #052-3131	• Failing to adequately disclose that adware which tracks and stores information regarding consumers' Internet use and displays advertisements based on that information is bundled with other software. • Installing adware, directly or through affiliates, on consumers' computers entirely without notice or authorization. • Failing to provide a reasonable or effective means for consumers to identify, locate, and remove adware from their computers.	Proposed settlement reached, ordering respondents to pay $1.5 million to the FTC. Respondents are forbidden from: • Displaying advertisements to any customer who obtained advertising software prior to October 1, 2005. • Exploiting security vulnerabilities in Internet browsers or other applications to install software. • Installing software without obtaining express consent from users. Respondents are obligated to: • Establish and publicize a consumer complaint mechanism that allows consumers to receive timely responses to their complaints about the advertising software. • Maintain a program to ensure that affiliates obtain proper consent from

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		consumers before installing software. • Identify the software program that causes advertisements to be shown to consumers on the advertisements themselves. • Provide links to the consumer complaint mechanism on the advertisements themselves. • Provide consumers with a reasonable means of uninstalling the advertising software. http://www.ftc.gov/os/caselist/0523131/index.htm

State Spyware Case Summary

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of New York v. Intermix Media, Inc. http://www.oag.state.ny.us/press/2005/apr/apr28a_05.html	• Deceptively and surreptitiously bundling invasive spyware or adware programs with "free" games, cursors, screensavers, or other small software programs. • Employing deceptive methods to prevent users from detecting and removing installed software, including: not making the software accessible in the "All Programs" or "Programs" list, hiding the software in folders not usually associated with programs, not listing the software in the "Add/Remove Programs" utility, not providing an uninstall utility for the software, and reinstalling the software after a user has deleted it.	New York General Business Law § 349, 350 New York common law prohibiting trespass to chattels	Settlement reached. Defendant agreed to pay $7.5 million in penalties and profit disgorgement, and accepted a ban on adware distribution. Founder and former CEO of Intermix also agreed to pay $750,000 in penalties and profit disgorgement. Acez Software, an affiliate which was downloading Intermix adware with free screensavers, agreed to pay $35,000. http://www.oag.state.ny.us/press/2005/oct/oct20a_05.html
State of Texas v. Sony BMG Music Entertainment http://www.oag.state.tx.us/oagnews/release.php?id=1370	• Failing to disclose on the packaging of an audio CD that software will be installed on the user's computer when the user places the CD in his computer. • Inducing the owner or operator of a computer to install software by ejecting an inserted audio CD unless the computer owner agrees to install the software, even though that software is not necessary for playback of the audio CD. • Surreptitiously installing a file that hides the presence of other files and folders such that the computer owner cannot locate them when performing a search of the file system. • Installing files and folders in a location on the	Consumer Protection Against Computer Spyware Act (Texas Business and Commerce Code § 48.001 *et seq*) Texas Deceptive Trade	Settlement reached. Defendant prohibited from releasing audio CDs containing software that employs technology to hide or cloak files or that does not provide an option to decline installation. Defendant required to provide notice on CD packaging of the functions and features of included software. Defendant's software is prohibited from gathering personal identifying information without users' express consent, and must be easily removed by users.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	computer such that the computer owner may confuse them for essential files needed to run the computer when this is not the case. • Failing to disclose the presence of a software component that hides other files and folders. • Installing software that remains hidden and active even when its associated music player software is not active. • Making it extremely burdensome if not impossible to remove software by not including an uninstall utility and by requiring the computer owner to contact customer service to remove the software. • Secretly installing files on a user's computer before the user has consented to the installation. • Leaving files secretly installed on a user's computer after the user has declined to accept the related software's EULA. • Failing to disclose to the user the presence of secretly installed files even after the user has declined to accept the related software's EULA. • Failing to provide an uninstall utility for files secretly installed before a user has consented to the installation.	Practices-Consumer Protection Act (Texas Business and Commerce Code § 17.47 *et seq*)	Defendant required to provide consumer redress and assistance by posting information on the Web, buying advertising to explain the content protection software's security vulnerability, and offering software patches. Defendant required to pay restitution to any consumer whose CD-ROM drive was disabled by the software. Defendant also obligated to pay $750,000 to the state of Texas for attorney's fees. http://www.oag.state.tx.us/oagnews/release.php?id=1889
People of the State of California v. Sony BMG Music Entertainment	• Failing to adequately disclose on the outer packaging of a CD or in its EULA that content DRM software would be required to be installed in order to use the CD on a computer. • Failing to adequately disclose that DRM software modifies the Windows operating system in ways unintended by Microsoft.	California Penal Code § 502(c) California Business and Professions	Settlement reached. Defendant is enjoined from: • Making false or misleading statements in connection with manufacture, sale or distribution of CDs. • Manufacturing or distributing any

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	• Failing to adequately disclose that DRM software uses cloaking technology to hide itself on users' computers. • Failing to adequately disclose that DRM software remains in operation at all times, consuming computer resources. • Failing to adequately disclose that DRM software connects to remote Internet servers. • Failing to adequately disclose that DRM software creates computer security vulnerabilities. • Failing to adequately disclose that DRM software cannot be accessed or removed without extraordinary computer sophistication or outside software. • Causing unauthorized software to be installed on users' computers.	Code § 17500	CD containing content protection software which hides or cloaks a file or directory. • Manufacturing or distributing any CD containing content protection software which is not readily removable through normal means. • Manufacturing or distributing any CD containing content protection software which tracks, limits or controls transfer or use of music files without disclosure on the outer packaging detailing features and limitations of the use of the CD. • Manufacturing or distributing any CD containing content protection software that tracks or collects personally identifiable information about users and which communicates such information to remote or another entity without express consent. Defendant required to provide consumer redress and assistance by posting information on the Web, buying advertising to explain the content protection software's security vulnerability, and offering software patches. Defendant required to pay restitution to any consumer whose CD-ROM drive was

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
			disabled by the software. Defendant also obligated to pay $750,000 to the state of California. http://ag.ca.gov/newsalerts/release.php?id=1400
State of Washington v. Secure Computer LLC, Paul E. Burke, Gary T. Preston, Manoj Kumar, Zhijan Chen, Seth T. Traub http://www.atg.wa.gov/pressrelease.aspx?&id=3770	• Intentionally using deceptive means to alarm the user that his computer may be infected with spyware and thereby inducing the user to download software that claims to be necessary to secure the user's computer. • Inducing the user to run a "free scan" of his computer through false representation and thereby transmitting software to the user's computer that deletes the user's "hosts" file. • Representing that software is an effective spyware removal program when it does not clean the user's computer of virtually any actual spyware. • Labeling something as spyware which is in fact a cookie or harmless registry key, or not installed on the computer at all. • Representing that a removal of infections has been performed when in fact the removed infections were harmless or not present and actual infections were not removed. • Trapping the user in a succession of pop-up warning messages and/or advertisements by simulating buttons on the pop-ups that normally permit the user to close windows or by altering the functionality of standard window-closing buttons.	Computer Spyware Act (Revised Code of Washington 19.270) Consumer Protection Act (Revised Code of Washington 19.86)	Defendant Chen admitted wrongdoing and agreed to pay $84,000 in fines and restitution as part of a settlement. The settlement prohibits Chen from sending Net Send messages for the purpose of advertising and from creating a false sense of urgency, exclusivity or need for products. Prior to advertising anything, Chen must consult with an attorney. Defendant Preston agreed to pay $7,200 in attorneys' fees as part of his settlement. The settlement prohibits him from assisting any person or organization in disguising its identity from the public or law enforcement. Defendant Traub agreed to a settlement in which he will pay $2,000 in attorneys' fees and refrain from illegally using trademarks, making unsubstantiated claims, or otherwise deceiving consumers in a marketing context. Defendant Secure Computer LLC agreed to pay $75,000 as restitution to Washington

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	• Engaging in other behaviors including misrepresenting software as a Microsoft product, violations of the CAN-SPAM ACT, and violations of Washington's Commercial Electronic Mail Act.		State purchasers of Spyware Cleaner and Pop-up Padlock, in addition to $925,000 in civil penalties and attorney fees. Settlement also prohibits defendant from engaging in numerous practices dangerous to consumers. http://www.atg.wa.gov/pressrelease.aspx?&id=5926
State of New York v. Direct Revenue, LLC, and Joshua Abram, Alan Murray, Daniel Kaufman, Rodney Hook http://www.oag.state.ny.us/press/2006/apr/apr04a_06.html	• Bundling a spyware program with "free" software without giving consumers any notice of the presence of spyware. • Bundling a spyware program with "free" software, giving consumers notice of the spyware only by following multiple links (in small print) through lengthy license agreements. • Distributing spyware through deceptive "ActiveX" advertisements that bombard consumers with pop-up prompts until they consent to a "free" software download that gives no notice of the presence of spyware. • Distributing spyware through deceptive "ActiveX" advertisements that bombard consumers with pop-up prompts until they consent to a "free" software download that gives notice of the presence of spyware only through a linked license agreement. • Installing spyware by using malicious code that exploits security vulnerabilities without giving any notice to consumers. • Displaying incessant pop-up ads, less than one minute apart, to consumers unwittingly infected with	New York Executive Law § 63(12) New York General Business Law § 349-350 New York common law	Litigation pending.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status

	spyware.
	• Displaying deceptive ads which promote "security" and "anti-spyware" programs to consumers unwittingly infected with spyware.
	• Distributing spyware that avoids detection and removal by:
	  o failing to inform consumers that the spyware has been installed,
	  o obfuscating the presence of the spyware by scattering its files across a user's computer, using randomly-generated file names, and ascribing false modification dates to the files,
	  o failing to uninstall the spyware when the software with which it was bundled is uninstalled,
	  o preventing the inclusion of the spyware in the Windows "Add/Remove Programs" utility, and
	  o reinstalling the spyware after consumers manually delete it.
	• Installing additional spyware and other programs after an initial spyware installation, without notifying consumers.
	• Installing additional spyware and other programs after an initial spyware installation, giving the spyware distributor permanent remote access to consumers' computers without their consent.
	• Failing to police contracted distributors, or to establish effective controls ensuring, promoting, or encouraging user notice and consent in third-party		

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	spyware distributions.		
State of Washington v. Software Online.com, and David W. Plummer[19]	• Misrepresenting the risk of harm to a user's computer (by falsely finding computers to be at risk and by listing Web sites to which the computer is vulnerable even when the computer blocks access to those sites) in order to induce the user to purchase a security product. • Misrepresenting the functions of standard "buttons" on software advertisements, thereby requiring users to continue to view the advertisements when they try to close them. • Leaving software files on users' computers without their knowledge or consent after they have uninstalled the associated software program. • Engaging in other behaviors including offering misleading negative-option billing to customers.	Consumer Protection Act (Revised Code of Washington 19.86.020)	Settlement reached in which defendants admit violations of the Consumer Protection Act. Defendants ordered to pay $150,000 in civil penalties and $40,000 in attorneys' fees. Settlement terms prohibit the following: • Inducing computer users to install software by misrepresenting that the user's computer is not secure. • Marketing software by means of a "free scan." • Using "buttons" in advertisements that do not function as the user would expect. • Installing software that causes pop-up ads when the user tries to close other ads. • Failing to provide a functional uninstall option. • Failing to obtain a consumer's explicit consent to purchase a product or service. http://www.atg.wa.gov/pressrelease.aspx?&id=3878

[19] An attorney for SoftwareOnline has disputed the inclusion of this case in this table. For more information, see the attorney's letter (http://www.cdt.org/privacy/spyware/20061208softwareonline.com.pdf) and CDT's response (http://www.cdt.org/privacy/spyware/20061222cdt.pdf).

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. Digital Enterprises, Inc., d/b/a Movieland.com; Alchemy Communications, Inc.; AccessMedia Networks, Inc.; Easton A. Herd; and Andrew M. Garroni http://www.atg.wa.gov/pressrelease.aspx?&id=4362	• Taking control of a user's computer by means of pop-up videos that the user cannot close out of and thereby obstructing the user's access to the computer and disabling the functionality of the computer. • Providing a software uninstallation option in the "Add/Remove" section of a user's computer which represents to the user that the software can be removed when in fact it cannot be removed. • Failing to disclose that the two practices listed above will be used to force the user to pay for software when the user's 3-day "Free Trial" of the software ends. • Failing to disclose that software downloaded onto a user's computer for a 3-day "Free Trial" will consume a significant amount of computer memory – at least 27 megabytes of RAM. • Failing to disclose that software will be transmitted to a user's computer surreptitiously and activated with the consumer's knowledge or permission. • Representing that software contains "no spyware" when the software itself constitutes spyware insofar as it places files on the user's computer which send repeated, harassing notices that interfere with use of the computer; prevents the user from uninstalling the offending files; and leaves parts of the software on the user's computer if he or she manages to uninstall it.	Unfair Business Practices—Consumer Protection Act (Revised Code of Washington 19.86) Computer Spyware Act (Revised Code of Washington 19.270)	Litigation pending.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. James Lane (QuikShield Security)	• Intentionally and knowingly deceiving consumers by stating that their computers have a malfunctioning security component and thereby inducing consumers to install security software. • Providing an uninstall process that does not work and does not remove the appropriate executable files from consumers' computers. • Misrepresenting that an advertisement for a commercial software product is a Microsoft operating system alert. • Misrepresenting that consumers have malfunctioning security components on their computers when no such components exist. • Misrepresenting the ability to close advertisements with "cancel" or "x" buttons when in fact those buttons open a web site associated with the advertisements. • Misrepresenting that a software product is "absolutely free" when in fact only five free uses of the product are available before consumers are forced to pay for further use.	Consumer Protection Act (Revised Code of Washington 19.86) Computer Spyware Act (Revised Code of Washington 19.270)	Settlement reached in which defendant agreed to pay $10,000 in civil penalties ($5,000 suspended pending compliance) and $6,444 in attorneys' fees. Settlement terms provide restitution to Washington residents and prohibit the following: • Failing to provide an operable install function for any products. • Misrepresenting the source of an advertisement. • Misrepresenting that security or privacy functions on a consumer's computer are not working properly. • Using the "X" button or other images typically associated with closing a window to perform any other function. • Failing to clearly identify the cost of a product. • Creating a false sense of urgency to purchase a product. http://www.atg.wa.gov/pressrelease.aspx?&id=4118

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. High Falls Media, LLC; Roc Telecom, LLC; Mark Libutti; Brian Einhaus; and Thomas A. Tortora (Spyware Slayer)	• Intentionally and knowingly using deceptive means to alarm consumers that their computers may be infected with spyware and thereby inducing consumers to install security software. • Misrepresenting that scanning a consumer's computer for spyware will not load any software onto the computer when in fact a software download is necessary to perform the scan. • Misrepresenting that a "99% chance" that a consumer's computer is infected has been detected when in fact nothing has been done to detect the presence of malicious programs on the consumer's computer. • Misrepresenting that certain registry keys on consumers' computers are "extreme risk" spyware when in fact the keys are harmless. • Failing to address consumers' software complaints. • Providing a disconnected telephone number for consumers to use for customer service. • Other behaviors involving deception and misrepresentation in violation of the Consumer Protection Act.	Consumer Protection Act (Revised Code of Washington 19.86) Computer Spyware Act (Revised Code of Washington 19.270)	Settlement reached in which defendants agreed to pay $300,000 in civil penalties ($275,000 suspended pending compliance) and $30,000 in attorneys' fees. Settlement terms provide restitution to Washington residents and prohibit the following: • Creating a false sense of urgency or need for a product. • Failing to respond to consumers' complaints. http://www.atg.wa.gov/pressrelease.aspx?&id=4950

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. SecureLink Networks LLC; NJC Softwares, LLC; Manuel Corona, Jr.; Rudy O. Corella; FixWinReg; and Hoanvinh V. Nguyenphuoc http://www.atg.wa.gov/pressrelease.aspx?&id=12328	• Installing a software bundle on a user's computer after the user has declined to consent to the bundle installation. • Failure to uninstall bundled software components when the program with which they came is uninstalled, or otherwise providing an obvious means of uninstalling bundled components. • Misrepresenting that advertisements for security software are operating system alerts regarding computer security problems. • Representing that critical security errors have been detected on a user's computer when no such errors were detected, with the purpose of inducing the user to purchase security products.	Computer Spyware Act (Revised Code of Washington 19.270) Consumer Protection Act (Revised Code of Washington 19.86)	Litigation pending.

Department of Justice Spyware Case Summary

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
United States v. Jerome T. Heckenkamp http://www.usdoj.gov/criminal/cybercrime/heckenkampPlea.htm	Prosecutors alleged: • Installing on another user's computer an unauthorized computer program that was designed to intercept electronic communications containing usernames and passwords. Defendant pled guilty to: • Engaging in other behaviors including gaining unauthorized access to a computer and recklessly causing damage to it.	18 U.S.C. §§ 2511(1)(a)	Count dismissed on government's motion (defendant convicted on separate, non-spyware counts). http://www.usdoj.gov/criminal/cybercrime/heckenkampSent.htm
United States v. Van T. Dinh	• Knowingly accessing a computer of another person without authorization by installing a series of "keystroke-logging" programs to remotely monitor the keystrokes of the computer user and thereby identify computer accounts and passwords.[20] • Engaging in other behaviors including a scheme to defraud an investor and committing mail and wire fraud.	18 U.S.C. §§ 1030(a)(4)	Defendant sentenced to 13 months in prison, ordered to pay $46,980 in restitution, and fined $3,000. http://www.usdoj.gov/criminal/cybercrime/dinhSent.htm
United States v. Juju Jiang http://www.usdoj.gov/criminal/cybercrime/jiangIndict.htm	• Knowingly accessing a computer of another person without authorization for the purpose of installing keylogging software to surreptitiously record keystroking activity on that computer and thereby collect computer usernames and passwords.[21] • Other behaviors involving trafficking in a counterfeit device and criminal infringement of copyrights.	18 U.S.C. §§ 1030(a)(4)	Defendant sentenced to 27 months in prison and ordered to pay $201,620 in restitution. http://www.usdoj.gov/criminal/cybercrime/jiangSent.htm

[20] Court documents for this case were unavailable online, thus the exact behaviors considered illegal by the Department of Justice were determined from supporting materials and press releases.
[21] *See* supra note 19.

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
United States v. Carlos Enrique Perez-Melara http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm	• Knowingly creating, possessing, and selling a computer program, knowing that the program is primarily useful for the purpose of surreptitious interception of electronic communications and that the program will be transported in interstate or foreign commerce. • Sending in interstate commerce the computer program described above. • Disseminating electronic advertisements for the computer program described above. • Intentionally promoting the use of the computer program described above for the purpose of surreptitious interception of electronic communications. • Knowingly intercepting wire communications using the computer program described above. • Knowingly disclosing to customers the contents of electronic communications obtained by using the computer program described above.	18 U.S.C. §§ 2512(1)(b), 2512(1)(a), 2512(1)(c)(i), 2512(1)(c)(ii), 2511(1)(a), 2511(1)(c)	Warrant issued for defendant's arrest.
United States v. John J. Gannitto (and the related cases of USA v. Powell, USA v. Selway) http://www.usdoj.gov/criminal/cybercr	Defendants pled guilty to: • Knowingly accessing a computer of another person without authorization by installing a computer program onto it and thereby obtaining information from the computer. Prosecutors also alleged: • Intentionally intercepting or procuring another person to intercept electronic communications of another person.	18 U.S.C. §§ 1030(a)(2)(c), 2511(1)(a)	Gannitto sentenced to 3 years supervised probation with 30 days in halfway house; Powell sentenced to 5 years supervised probation; Selway sentenced to 3 years unsupervised probation. Each defendant

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
ime/perezIndict.htm			sentenced to pay a $500 fine.
United States v. Cheryl Ann Young http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm	Defendant pled guilty to: • Intentionally intercepting or procuring another person to intercept electronic communications of another person. Prosecutors also alleged: • Knowingly accessing a computer of another person without authorization by installing a computer program onto it and thereby obtaining information from the computer via interstate or communication with it.	18 U.S.C. §§ 1030(a)(2)(c), 1030(c)(2)(B)(ii), 2511(1)(a)	Defendant sentenced to 3 years probation and ordered to pay a $500 fine and a $100 special assessment. Defendant ordered to perform 100 hours of community service and refrain from contact with victim.
United States v. Christopher Maxwell http://www.usdoj.gov/criminal/cybercrime/maxwellIndict.htm	• Creating and using Internet Relay Chat botnets remotely and surreptitiously to install adware or other unauthorized programs on thousands of compromised computers, without the knowledge or consent of the computers' owners, and thereby obtaining thousands of dollars in commission payments from adware companies for those installations. • Conspiring to do the above.	18 U.S.C § 371, 18 U.S.C §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(ii)	Defendant sentenced to 37 months in prison and forced to pay $252,000 in restitution and a $200 special assessment. http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm
United States v. Jeanson James Ancheta http://www.usdoj.gov/criminal/cybercrime/anchetaArrest.	• Knowingly gaining unauthorized access to thousands of computers with the intent to install adware on those computers without notice to or consent from the users, and thereby obtaining thousands of dollars from the adware companies. • Redirecting infected botnet computers to a server containing a Trojan horse program and thereby causing the surreptitious installation of adware on the infected computers.	18 U.S.C § 371, 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v)	Defendant sentenced to 57 months in prison, forced to pay $15,000 in restitution and forfeit the proceeds from his illegal activity. http://www.usdoj.gov/crimina

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
htm	• Conspiring to do either of the above. • Engaging in other behaviors including conspiring to obtain unauthorized access to thousands of computers and launching denial of service attacks.		l/cybercrime/anchetaSent.htm
United States v. Kenneth Kwak http://www.usdoj.gov/criminal/cybercrime/kwakPlea.htm	• Intentionally installing remote control software on a user's computer (in a United States department or agency) with the intention of observing and gaining unauthorized access to that user's Internet use, electronic mail, and computer files. • Intentionally using remote control software to alter settings and defeat password protections on a user's computer (in a United States department or agency), thus allowing unrestricted access to the user's email by other persons on the user's network.	18 U.S.C. §§ 1030(a)(2)(B), 1030(c)(2)(B)(ii)	Defendant sentenced to 5 months in prison followed by 5 months of house arrest and ordered to pay $40,000 in restitution. http://www.usdoj.gov/criminal/cybercrime/kwakSent.htm
United States v. George Nkansah Owusu	• Surreptitiously installing a keylogger program on public computers to record every keystroke made on those computers and using the collected data to gain unauthorized access to users' online accounts and university management systems.[22]	18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(ii)	Defendant sentenced to 4 years in prison followed by 4 years supervised release and ordered to pay $2,550 in restitution.

[22] See *supra* note 20.

Mr. RUSH. Thank you.

Our next witness, and Mr. Cerasale, if I mispronounce your name, please correct me, is Mr. Jerry Cerasale, a senior vice president of government affairs for the Direct Marketing Association Incorporated, DMA. DMA represents 3,600 member companies that are engaged in direct database and interactive marketing and electronic commerce. Last year the association developed and adopted standards for software downloads as part of its guidelines for ethical business practice. DMA opposes this bill and a broad regulatory approach in general because it believes that self-regulation coupled with existing FTC authority is working to crack down on harmful spyware.

Mr. Cerasale, you are recognized for 5 minutes.

STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

Mr. CERASALE. Thank you very much, Mr. Chairman. With a last name like mine, I respond to anything that comes close. So that is fine. Cerasale is how it is pronounced but Cerasale is all right as well. I am not ashamed of my heritage.

I do thank you for inviting us here and I would ask that my written testimony be placed in the record, and I thank you for recognizing DMA, the leading trade association. We have been around since 1917 and our members are part of the economy, very much part of this new e-commerce as they are providers of Internet service. They sell goods on the Internet and so forth. This is very important for us.

We agree fully with the subcommittee and the committee that we want to try and rid the Internet of spyware. That is really a goal that I think we should all be working toward, and I want to commend this committee especially because you were the instigator. You were the catalyst for moving forward in trying to get industry looking at spyware. You were the catalyst to DMA in producing our guidelines for spyware, for downloading of software on the computers. You were the catalyst for browsers taking any spyware software and putting it in their browser. You are the catalyst for computer manufacturers adding that onto computers. You are the catalyst for software providers creating anti-spyware software. And I believe you are the catalyst for the FTC and the States for moving and trying to go against those bad actors putting on spyware deceptively onto consumers' computers and stealing information, stealing their computer, slowing it down and forcing those many people who had to throw away their computers.

We have made progress since you started this investigation. It is not over, and I don't think it will ever be over. As technology changes, bad actors adapt. They get new technology and we are going to have to be ever vigilant as we go forward here. We don't think at the DMA that there is really a magic bullet that is an all-purpose answer to everything here, which is why we look at going forward with our guidelines because we can change them fairly rapidly and try and adjust to what is happening in the marketplace and try and keep this Internet open for e-commerce.

We are really pleased that e-commerce has grown. One of the great things is as we look at the growth, we have statistics to show it is growing at 24 percent right now. It had been larger but it is continually growing, and one of the great things was that Cyber Monday was larger than Black Friday this holiday season and the gap is going to get larger and larger as e-commerce becomes more and more part of our American experience for the benefit of consumers and the benefit of businesses.

As we look at H.R. 964, we support granting the attorneys general the opportunity to and the authority to enforce the law. We think that is a major part of balancing for preemption. We also support the efforts and what is in section 2 of the law. We think going after the bad actors is really what is important and strikes the right balance.

We have some concerns with section 3 of the bill. We think that the broad definition of software, and we had a very difficult time trying to define software in our guidelines so it is not something that is new. A broad definition of software will take into account and cover things that are part of the seamless use of the Internet that Americans are used to, that provides advertising-supported contents, there is so much free content on the Internet and so we think that section 3 probably goes further than we would want. We believe you need conspicuous notice, you need choice for the consumer, you need an ability to uninstall or at least totally disengage, disable any software that is put on your computer. We think there should be a link to the privacy policy of the person putting on the software and the name of the company should be known. We think that strikes the balance for consumer choice plus advertising marketing-supported Internet content which is available free to most Americans.

The DMA has a concern with the Good Samaritan provision. We are worried that the Good Samaritan provision in the bill could become a means, an anti-competitive means and so we want to make sure that we look at that and strike that balance and make sure that is there. We also think that the monitoring provision in 5(b) is a little bit too narrow. That provision for the anti-fraud thing looks at certain companies. There are other companies that do anti-fraud that aren't covered in that exemption and we think that they are there.

We want to thank you very much for having me here today.

[The prepared statement of Mr. Cerasale follows:]

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

HOUSE ENERGY & COMMERCE COMMITTEE

HEARING ON

COMBATING SPYWARE: H.R. 964, THE SPY ACT

MARCH 15, 2007

TESTIMONY OF

JERRY CERASALE
SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS

ON BEHALF OF

DIRECT MARKETING ASSOCIATION, INC.

Jerry Cerasale
Senior Vice President, Government Affairs
Direct Marketing Association, Inc.
1615 L Street, NW Suite 1100
Washington, DC 20036
202/955-5030

I. Introduction & Summary

Good morning Mr. Chairman and members of the Subcommittee. I am Jerry Cerasale, Senior Vice President for Government Affairs of the Direct Marketing Association, and I thank you for the opportunity to appear before the Subcommittee as it examines H.R. 964 and the spyware issue in general.

The Direct Marketing Association, Inc. ("DMA") (www.the-dma.org) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing, promotes relevance as the key to reaching consumers with desirable offers, and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, DMA today represents more than 3,600 companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

DMA and our members appreciate the Committee's continued outreach to the business community on this important issue. I note at the outset that this is a complicated issue; there is no panacea that can fully solve it. In part due to the Committee's attention, over the past two years there have been significant developments that have fundamentally improved the consumer experience as it relates to spyware. Where once, just two short years ago, pop-up ads, drive-by downloads, and software that hijacked computers were on the rise, consumers in 2007 experience fewer such unwanted practices. Industry guidelines for legitimate software downloads, strong self-regulation, major technological improvements, and Federal Trade Commission ("FTC") and state Attorney General enforcement have all contributed to the current, significantly improved environment where the prevalence of spyware has been vastly reduced. While DMA supports the Committee's interest in combating spyware, we do not believe that a broad regulatory approach to all software downloads and Internet marketing as set forth in Section 3 of this bill is the appropriate approach to this issue and is not in the best interest of either consumers or business.

DMA is particularly concerned that this legislation could negatively impact legitimate advertisers and marketing practices that are critical drivers of the Internet economy. Internet growth over the past 10 years has been nothing short of remarkable, and this growth is fueled by advertising and marketing. The dramatic rise of the Internet is evident in the dollar amounts consumers spend purchasing products through Internet sales. This year, on Cyber Monday, nearly 30 million shoppers spent more than $608 million in just one day. The numbers are up 26% from the same day last year and are more than the amount shoppers spent on Black Friday.

The U.S. Census Bureau, which releases quarterly retail e-commerce statistics, recently reported that estimated retail e-commerce sales for the 4th quarter of 2006 were $29.3 billion, an increase of 6.3% from the 3rd quarter of 2006, and an increase of 24.6 percent from the 4th quarter of 2005. It also noted that 4th quarter e-commerce sales accounted for 3.0% of total sales.[1] comScore Networks reported that for calendar year 2006, online retail spending reached $102.1 billion, a 24% increase from 2005.[2]

As these and similar figures suggest, the Internet revolution has had a tremendous impact on economic growth. The Internet has become a preferred mechanism of commerce for many consumers, and a key part of multi-channel sales efforts for businesses. This phenomenon has changed the way products and services reach the market, and enables consumers to shop in an environment that knows no restrictions on time or place.

II. Strong Guidelines, Technology, and Enforcement Have Reduced the Need for Legislation

The combination of strong industry guidelines, anti-spyware technologies, and enforcement of existing laws over the past two years has limited pernicious software downloads. Specifically, spyware's threat to the positive consumer experience online has been reduced. Together, we are winning the battle against such malicious practices. This said, this battle will be ongoing. Today's solutions and remedies may be obsolete tomorrow. As technology

[1] U.S. Census Bureau. *Quarterly Retail E-commerce Sales, 4th Quarter 2006*, February 16, 2007. *See* http://www.census.gov/mrts/www/data/html/06Q4.html.

[2] *See* http://www.comscore.com/press/release.asp?press=1166.

continues to evolve rapidly, so too will the challenges posed by spyware and related bad practices.

A. Industry Guidelines

DMA has long been a leader in establishing comprehensive self-regulatory guidelines for its members on important issues related to privacy and e-commerce, among many others. DMA and its member companies have a major stake in the success of electronic commerce and Internet marketing and advertising, and are among those benefiting from its growth. Our members understand that their success on the Internet is dependent on consumers' confidence in the online medium, and support efforts that enrich a user's experience while fostering consumer trust in online channels. Understanding the importance of standards and best practices in building consumer confidence, DMA, working with its members, in 2006 developed and adopted Standards for Software Downloads as part of our Guidelines for Ethical Business Practice ("Guidelines"), to specifically discourage illegitimate software download practices that threaten to undermine electronic commerce and Internet advertising.[3] In our experience, industry guidelines are the most effective way to address the continuously changing technological landscape. Such guidelines are flexible and adaptable in a timely manner so as to cover bad practices and not unintentionally or unnecessarily cover legitimate actors.

DMA requires member organizations to adhere to this Guideline, which encourages members to provide notice and choice regarding software that may be downloaded onto a consumer's personal computer or similar devices. The Guideline clearly states that marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include software that takes control of a computer, modem hijacking, denial of service attacks, and endless loop pop-up advertisements. The Guideline also is clear that businesses should not deploy programs that deceptively modify or disable security or browser settings or prevent the user's efforts to disable or uninstall the software.

---

[3] Use of Software or Other Similar Technology Installed on a Computer or Similar Device, DMA Guidelines for Ethical Business Practice, at 21 (attached) (available at http://www.the-dma.org/guidelines/EthicsGuidelines.pdf).

The Guideline also details responsible practices for marketers offering software or other similar technology that is installed on a computer used to further legitimate marketing purposes. Specifically, such programs must provide a user with clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects of having the software or other similar technology installed. Marketers also must give the user an easy means to uninstall the technology and/or disable all functionality. Finally, marketers should always provide an easily accessible link to privacy policies and contact information, as well as clear identification of the company making the offer.

Given the rapid evolution of technology, DMA believes that self-regulation is the most effective means for setting business standards for legitimate marketing. Guidelines like those published by DMA and TRUSTe, about which you will hear today, condemn deceptive practices, strive to protect consumers, and foster legitimate Internet advertising and marketing. Guidelines are flexible and adaptable to changes in markets, business practices, and advances in technology.

Another issue that DMA has sought to address through self-regulatory best practices is the role of advertisers in ensuring that their advertisements are being disseminated responsibly. In some instances, there may be advertisers with good intentions who do not understand where their ads are appearing online. To help address some of these issues, last year DMA adopted best practices regarding online advertising networks and affiliate marketing.[4] These best practices state, among other things, that marketers should obtain assurances that their partners will comply with legal requirements and DMA's Ethical guidelines, undertake due diligence in entering into these partnerships, define parameters for ad placement, and develop a monitoring system for online advertising and affiliate networks. These should limit the appearance of advertisements related to spyware.

B. Current Law Enforcement Efforts

Technology, self-regulation, and existing laws and enforcement are adequately addressing the problems caused by spyware. In the past couple of years, law enforcement

[4] *See* DMA Best Practices for Online Advertising Networks and Affiliate Marketing (attached) (available at http://www.the-dma.org/guidelines/onlineadvertisingandaffiliatenetworkBP.pdf).

officials have been using existing enforcement tools to pursue sources of spyware. The FTC has aggressively pursued adware companies engaging in improper business practices. Since 2004, it has brought more than 10 such cases under its deceptive and unfair practices authority.[5] In addition, the Department of Justice ("DOJ") is actively combating spyware under the Computer Fraud and Abuse Act and the Wiretap Act, also with more than 10 cases to date.[6] The states have been an important part of the enforcement efforts in this area as well, with state attorneys general using their fraud and consumer protection laws to target distributors of spyware.[7] Strong enforcement of existing laws, combined with industry self-policing and innovative technologies, thus has drastically slowed the spread of spyware and its effects. As these efforts indicate, continued dedication of resources to enforcement has proven an effective response to spyware.

C. The Marketplace Technology Adopted to Combat Spyware

The technological tools available to consumers to prevent spyware also have seen significant improvement in their effectiveness. These tools are highly sophisticated, user friendly, and widely available, and in many instances are at no cost to the consumer. For instance, today's anti-spyware software is proactive in detecting malware before it can penetrate a consumer's personal computer, thereby eliminating frustrations of spyware by preventing it from ever being downloaded. Consumers also have access to new web browsers with stronger security features and better warning features. In addition, as spyware became a problem, industry responded by installing anti-spyware software onto personal computers before shipping them to customers. This service provides personal computers with an early vaccination against spyware.

---

[5] *See, e.g., In the Matter of DirectRevenue LLC*, FTC File No. 052-3131 (filed Feb. 16, 2007); *In the Matter of Sony BMG Music Entertainment*, FTC File No. 062-3019 (filed Jan. 30, 2007); *FTC v. ERG Ventures, LLC*, FTC File No. 062-3192 (filed Nov. 29, 2006); *In the Matter of Zango, Inc. f/k/a 180Solutions, Inc.*, FTC File No. 052-3130 (filed Nov. 3, 2006).

[6] CFAA, 18 U.S.C § 1030; Wiretap Act, 18 U.S.C § 2511. *See, e.g., U.S. v. Jerome T. Heckenkamp*, http://www.usdoj.gov/criminal/cybercrime/heckenkampSent.htm; *U.S. v. Christopher Maxwell*, http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm.

[7] For example, New York attorneys general over the past few years, and other attorneys general, have been actively pursuing cases against companies for deceptive practices in connection with spyware and adware. *See* NY AG settlement with online advertisers, http://www.oag.state.ny.us/press/2007/jan/jan29b_07.html; settlement with Direct Revenue, http://www.oag.state.ny.us/press/2006/apr/apr04a_06.html.

III. Specific Concerns about H.R. 964

I would like to take this opportunity to describe specific comments regarding H.R. 964, which is pending before the Subcommittee. Although DMA is aware that similar legislation passed the House in each of the last two Congresses, we believe that the significant developments we described warrant reevaluation of certain provisions of this legislation, which we hope that the sponsors of this bill and the Subcommittee will consider.

First, DMA has significant concerns about Section 3 of the bill, and is concerned that it would limit current and future critical Internet offerings. For this reason, DMA believes that Section 3 should be tailored to target defined bad practices, rather than create regulation of many legitimate information practices resulting from software. The current language in Section 3 extends beyond regulating "surreptitious surveillance" practices and would apply notice and consent to all "information collection software," defined to include software that collects personally identifiable information or non-identifiable information used for advertising purposes. DMA and its membership have long supported the principle of notice and choice surrounding the use of personally identifiable information. However, requiring notice and consent for all information practices tied to software downloads would result in limiting the consumer's Internet experience. The proposed requirements would prove an obstacle to consumer personalization and customization of websites as consumers would eventually cancel requests to transmit information, without first learning of the program's purpose, missing the opportunity to obtain unique and valuable tools that could enrich their online experiences. This would all culminate in a restraint on innovation and the deployment of new, seamless technologies.

DMA also is concerned about the possible consequences from a provider acting under the "Good Samaritan" protection in Section 5. This provision, unlike prior proposals, would limit liability for violations "under this Act" for providers of anti-spyware software that remove spyware from a computer. This provision is far narrower than previous proposals that would have limited liability for such providers for any removal of software.

The policy goal underlying the current Good Samaritan proposal is unclear. The operative provisions of Sections 2 and 3 would impose liability for placing software on a machine, not removing software. Thus, it is unclear why a provision limiting liability for

"removal" of software is necessary. If the Committee's goal is to not impose liability on entities that place anti-spyware software on a computer, a more appropriate approach would be to exempt providers of such software from the definition of "information collection software" in the first instance. Given the circumstances surrounding this provision and the fact that it is limiting liability where none exists in the first instance, DMA suggests that the provision be removed.

Although DMA supports a provider's ability to remove or disable a program employed to perpetrate a bad act, we are apprehensive that a broader "Good Samaritan" provision would empower providers to remove legitimate software from a customer's computer and thus raises competitive concerns. Program removal can be a complex procedure with unintended negative effects, especially when the software cannot be isolated. A forced removal may cause other legitimate programs to improperly function or not function at all. In the end, the consumer would suffer. The current framework, under which existing laws are used to hold anti-spyware companies liable for removal of legitimate software, has served as an important check on overreaching of such programs and should be preserved.

Finally, DMA believes that Section 5(b), which provides immunity to the specified entities for monitoring undertaken for purposes including security and fraud detection and prevention, is drafted too narrowly and should be extended to cover the activities of entities beyond those enumerated that engage in fraud prevention activities. For example, DMA member companies, including information service providers acting on another company's behalf (e.g., online retailer), are involved in financial transactions, such as extending credit. When a consumer applies for credit, these member companies provide critical fraud prevention tools that must operate seamlessly with the overall process. To isolate such an anti-fraud tool would undermine the overall security of the online transaction. For these reasons, Section 5(b) should be more broadly drafted to include other vital anti-fraud activities.

IV. Conclusion

In summary, the combination of advances in industry self-regulation, FTC enforcement, and technology, coupled with concerns about interfering with legitimate uses of software for marketing purposes, necessitates that Section 3 be revisited. If regulation is necessary, it should

be drafted in manner that does not undermine current efforts or upset consumers' expectations regarding the types of available, legitimate online marketing.

Thank you for your time and the opportunity to speak before your Subcommittee. I look forward to your questions and working with the Subcommittee on this legislation.

Excerpt from the DMA Guidelines for Ethical Business Practice

USE OF SOFTWARE OR OTHER SIMILAR TECHNOLOGY INSTALLED ON A COMPUTER OR SIMILAR DEVICE
Article #40
Marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include, but are not limited to, software or other similar technology that:

- Takes control of a computer (e.g., relaying spam and viruses, modem hijacking, denial of service attacks, or endless loop pop-up advertisements)
- Deceptively modifies or deceptively disables security or browser settings or
- Prevents the user's efforts to disable or uninstall the software or other similar technology

Anyone that offers software or other similar technology that is installed on a computer or similar device for marketing purposes should:

- Give the computer user clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects* of having the software or other similar technology installed
- Give the user an easy means to uninstall the software or other similar technology and/or disable all functionality
- Give an easily accessible link to your privacy policy and
- Give clear identification of the software or other similar technology's name and company information, and the ability for the user to contact that company

*Determination of whether there are significant effects includes, for example:

- Whether pop-up advertisements appear that are unexpected by the consumer
- Whether there are changes to the computer's home page or tool bar
- Whether there are any changes to settings in security software, such as a firewall, to permit the software to communicate with the marketer or the company deploying the software, or
- Whether there are any other operational results that would inhibit the user's expected functionality

Cookies or other passive means of data collection, including Web beacons, are not governed by this Guideline. Article #37 provides guidance regarding cookies and other passive means of data collection.

DMA's Internet Marketing Advisory Board (IMAB)
Best Practices for Online Advertising Networks and Affiliate Marketing

Online marketers using advertising and affiliate networks should:

1. Obtain assurances that the online advertising and affiliate network is in full compliance with state law, federal law, and the DMA Guidelines for Ethical Business Practice.
2. Perform due diligence on prospective network advertising partners and make sure you are working with reputable firms. Additionally (if possible), obtain a sample list of current advertising clients. Due diligence should also include either 1) asking for a full disclosure of eligible sites, or 2) a review of processes to limit access to unwanted sites or channels. When partnering with an aggregate site online advertising and affiliate networks should provide the marketer with a sampling of sites that are in their network. Due diligence should encompass the entire process from the marketer to the end consumer.
3. Always utilize a written contract/agreement. This will provide you the greatest possible control over your ad placement. This will also be the mechanism by which you devise and enforce formulas and/or guidelines for where and how online ads will be placed.
4. Include specific parameters that must be employed to determine placement of your online ads in written agreements. Altering of offer by an advertising or affiliate network is prohibited. If laws, guidelines or set standards are violated your contract with the violating advertising or affiliate network should be terminated.
5. Develop a system to routinely monitor your ad placements as well as your contract with any online advertising or affiliate network.

June 2006

Mr. RUSH. Our next witness is Mr. Dave Morgan. Mr. Morgan is the founder and the chairman of TACODA, Incorporated. Mr. Morgan will testify on behalf of his company and on behalf of the Interactive Advertising Bureau, which represents more than 300 leading companies that are responsible for selling more than 86 percent of online advertising. TACODA, which develops innovative technologies for target marketing, says on page 4 of its written statement that it supports H.R. 964, the next three pages detailing its complaints against everything but section 2.

Now we will recognize Mr. Morgan for 5 minutes.

STATEMENT OF DAVE MORGAN, FOUNDER AND CHAIRMAN, TACODA, INC.

Mr. MORGAN. Thank you. Chairman Rush, Ranking Member Stearns and members of the subcommittee, thank you very much for inviting me to testify on H.R. 964.

I am Dave Morgan, and as you can tell, I am wearing two hats here today. One is the founder and chairman of TACODA, Inc., a New York-based online advertising company, and also as the chairman of the Public Policy Council of the Interactive Advertising Bureau, which is the trade body of basically the largest majority of the online advertising today.

Consideration of this legislation in past Congresses has been an extraordinarily open and bipartisan effort and we welcome the opportunity to participate with the committee and the staff in developing appropriate language that balances consumer protection with fostering continued growth on the Internet. It is clear to me and the IAB that this subcommittee intends to address the legislation to combat purveyors of malicious software while at the same time not adversely affecting legitimate online practices such as those employed at TACODA.

The consumer experience with respect to spyware and online advertising has improved in the last few years and I would say I think the primary driver of that has been this committee's focus on the issue and the clear intent that the bad practices and this kind of action will not be tolerated. Second, we have certainly seen significant prosecutions and actions from the Federal Trade Commission and we have also seen a lot of industry self-regulatory effort, and as a member of the industry, I can tell you much of that has also been driven from a reaction from your attention to this issue, and also the self-regulation in areas of downloadable software. Given these developments and particularly with respect to the broader online advertising industry, we do think that there are issues around section 3 where there could be some unintended consequences.

A little bit about TACODA. It was created in 2001 as a company to target online advertising. We deliver billions of advertisements online every day in the pages of major Web sites like the New York Times or Chicago Tribune or Orbitz, not pop-up advertising and the protection of consumer privacy and the principles of relevancy, transparency and freedom of choice have been hallmarks of TACODA's business practices from the beginning. We are a board member of the Network Advertising Initiative, the NAI, the Direct

Marketing Association and its interactive marketing advisory board.

Interactive and online advertising is the primary means of funding a cost-free rich Internet as well as free access to unparalleled products and services. Online advertising is paying the bills for what people are spending more than 20 percent of all of their media consumption today. TACODA and the IAB have worked closely with Web sites to develop guidelines to address topics including e-mail, popup ads, lead generation. Most people are probably surprised by the impact of online advertising and the fact that it is supporting this content but that is the reality because the vast majority of the content online is free today because advertising has paid for it.

We support H.R. 964's efforts to combat spyware. We strongly agree that spyware is bad for consumers, business and the online advertising industry. The bill does not impinge on certain legitimate practices like those of TACODA which make it very easy at TACODA to be supportive of this legislation. But there is always a risk of legislation that governs technology and technology practices and that is where there are the areas of concern across the broader industry, that there may be some unintended consequences of defining technology, and given the dramatic advances in combating spyware and the guidance now available from enforcement and self-regulatory initiatives that did not exist at the outset of the last Congress, we believe that certain provisions of the bill are worth re-examining: the broad definitions of computer software and personally identifiable information as well as requirements in connection with the collection of both personal information and non-personal information. In addition, there are new technologies that really weren't even utilized as recently as 2 years ago in areas of some certain uses of cookies and java and java script.

Additionally, the IAB hopes to ensure that the anti-spyware providers can continue to remove bad software. We recognize the goal of the Good Samaritan provision. However, we would have concerns that with changes that have broadened this language to create a more extensive immunity provision, that would afford companies broad discretion to remove legitimate software which is often misidentified as spyware.

Thank you for considering the views of TACODA and the IAB on these issues. The success of the Internet has helped fuel this country's economy. We look forward to working together with you. Thank you, Chairman Rush. Thank you, Ranking Member Stearns. Thank you, members of the subcommittee. I look forward to your questions.

[The prepared statement of Mr. Morgan follows:]

TESTIMONY BEFORE THE
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
H.R. 964, "SECURELY PROTECT YOURSELF AGAINST CYBER TRESPASS ACT"
ENERGY AND COMMERCE COMMITTEE
U.S. HOUSE OF REPRESENTATIVES
THURSDAY, MARCH 15, 2007
BY
DAVE MORGAN
FOUNDER & CHAIRMAN OF TACODA, INC.
ON BEHALF OF THE INTERACTIVE ADVERTISING BUREAU

Chairman Rush, Ranking Member Stearns, and members of the Subcommittee – thank you very much for inviting me to testify on H.R. 964, the "Securely Protect Yourself Against Cyber Trespass Act." My name is Dave Morgan and I am here today wearing two hats. First, I am the founder and chairman of TACODA, Inc., a six-year-old New York-based online advertising company that has been a pioneer both in targeted online advertising as well as consumer privacy protection. I am also here today as Chairman of the Public Policy Council of the Interactive Advertising Bureau ("IAB"). Founded in 1996, the IAB represents more than 300 leading interactive online companies that are actively engaged in, and support the sale of, interactive and online advertising. Some members include Yahoo, AOL, MSN, Google, Forbes.com, New York Times Digital, and CNET Networks. IAB membership is responsible for selling more than 86% of interactive and online advertising in the United States. On behalf of its members, the IAB evaluates and recommends standards and practices, fields interactive effectiveness research, and educates the advertising industry. IAB opened a Washington, D.C. office this year to oversee regulatory matters, legislative affairs, and public policy initiatives that affect the interactive and online advertising industry.

Consideration of this legislation in past Congresses has been an extraordinarily open and bi-partisan effort. We have welcomed the opportunity to participate with the Committee and staff in developing appropriate language that balances consumer protection with fostering continued growth of the Internet. I look forward to sharing both my company's and the IAB's members' experiences and insights with the Subcommittee. It is abundantly clear to me that the Subcommittee intends this legislation to combat purveyors of malicious software. At the same time, it is clear that this legislation is not intended to affect legitimate online practices such as those employed at TACODA.

At the outset, I want to highlight that since this legislation was first introduced in the 108th Congress, the consumer experience as it relates to spyware and online advertising has improved. This is due to several significant developments. First, a primary driver for improvement was the Committee's focus on this issue, and its clear indication that bad actors online will not be tolerated. Second, the Federal Trade Commission and state enforcement authorities have, in their law enforcement activities and settlements, given industry fairly clear guidelines on what is and is not acceptable under existing law. Third, and as others on the panel will describe, industry self-regulation has played a significant part in defining the rules of the road for downloadable software. Given these developments, we believe that certain provisions of the legislation, and particularly Section 3, merit a renewed look.

Let me start by telling you a little bit about TACODA. Created in 2001, TACODA is an interactive and online advertising company based in New York City with offices in Dallas, Chicago, Los Angeles, and Seattle – among others. TACODA is the largest and most advanced online ad targeting network in the world. We safely and effectively deliver hundreds of billions of relevant banner ads each month for companies such as Coca-Cola, HP, Sony, Microsoft, and American Express. These ads are delivered as "in-page" or "embedded" ads – not pop-ups – within the pages of more than 4,500 of the most recognized Web sites on the Internet. Some include the sites of The New York Times, NBC Universal, Cars.com, The Dallas Morning News, and the Associated Press. This synergy produces a better experience for consumers, more effective and more efficient advertising for marketers, more revenue, higher yields, and improved consumer loyalty.

The protection of consumer privacy and the fundamental principles of relevancy, transparency, and freedom of choice have been hallmarks of TACODA's business practice. Consumer privacy and data protection are essential to our business success, and TACODA is the unquestioned leader in "safe targeting." TACODA leverages its "safe targeting" technology on partner Web sites to collect only anonymous, non-identifying information and group visitors into segments that are relevant for advertisers. These visitors then receive advertising most relevant to their interests whenever they visit a Web site with which TACODA has a relationship.

TACODA is a leader in working with industry in developing best practices and self-regulatory guidelines. It is a board member of the Network Advertising Initiative (the "NAI"), and an active member of the Direct Marketing Association ("DMA") and its Interactive Marketing Advisory Board.

In November of last year, TACODA announced its "Consumer Choice Initiative" to go even farther than regulations or industry best practices requirements for protecting consumer privacy. Specifically, TACODA:

- Collects only anonymous, non-identifying information.
- Notifies every consumer who participates in its network at least once every six months and gives them a chance to opt out of receiving ads from the TACODA network.
- Developed patent-pending technology to recognize a consumer's opt-out status even in instances where they have deleted their browser cookies. This technology was designed to preserve consumer choice.
- Actively monitors content, to help protect against associating branded advertising with inappropriate content.

Now, I would like to talk about the industry more broadly. Interactive and online advertising is a primary means of funding for cost-free, rich Internet content, as well as free access to unparalleled products and services. Such advertising has lowered barriers to market entry, enabling new businesses, both small and large, to thrive. Internet advertising and commerce has enabled local businesses – from antiques dealers to auto dealers, to reach national markets. Consumer confidence in online channels is critical to the vitality of the interactive and online advertising industry. Thus, we take very seriously all issues that affect the consumer relationship, including legitimate software downloads that are used for advertising practices. Recognizing the importance of industry standards and best practices to ensure continued consumer confidence in the online medium, TACODA and the IAB have worked closely with Web sites to develop guidelines to address topics including e-mail, pop-up ads, and lead generation. Self-regulatory efforts, especially in the context of the Internet and interactive and online advertising, are an extremely effective and efficient means to promote legitimate practices and marginalize bad actors. For example, TACODA is in full compliance with the NAI principles, which have been applauded by the FTC and provide a self-regulatory framework for the practice of interactive and online preference-based marketing.

Many people are probably surprised by the impact that interactive and online advertising has already had in the marketplace in its still very short existence. The vast majority of the content on the Internet today – free news, entertainment, and information – is supported primarily by interactive and online advertising. Consumers do not pay for this. Telecommunication service companies do not pay for this. Online advertising bears a great majority of these costs.

Free content is enriching lives in rural America, urban America, among immigrants, and among the very poor. I grew up in a small town in western Pennsylvania. The only way to get a printed copy of The New York Times is to order it at least two days in advance and to pay $5 per copy. Needless to say, not many people in my town can afford to read "All the News That's Fit to Print." Now, because of the Internet and ad-supported content, everyone in town can read it for free, either through their Internet access or on a computer at the Shaw Public Library. Without having to pay for printing presses and trucks, our industry is supporting diverse voices and views across our land and around the world. These new voices are keeping traditional media honest and in tune with the local communities. These new outlets permit government entities and public officials to speak directly to their constituents, without filters and bias. These new online platforms are supporting the efforts of millions of small businesses and home businesses, giving them access to global markets. For example, eBay helped created hundreds of thousands of new small businesses and home businesses and they are 100% dependent on interactive and online advertising and e-commerce.

Now, let's talk specifically about H.R. 964. We at TACODA support efforts to combat spyware, the underlying impetus of the bill. We strongly agree that spyware is bad. It is bad for consumers and bad for business. It can infect their machines with malicious software and remove the ability of consumers to exercise choice on their computers. Spyware is equally bad for the interactive and online advertising industry. It makes consumers suspicious when online. This, in turn, makes advertisers more wary to invest their marketing efforts in online channels. I don't think that anyone on the panel disagrees.

We have worked diligently with the Committee staff since the bill's first introduction to ensure that the bill does not impinge on certain legitimate practices like those of TACODA. For that reason, it is easy for TACODA to support the bill. That said, there is always a risk that legislation that governs complicated technology could result in limiting and/or stifling innovation, which we know the Committee does not want. However, as someone who has worked in this industry for more than 15 years, since before we even had Web advertising, and as a designated representative of the IAB, I should also inform you that there are provisions in the bill as currently drafted that could have some broad and unintended consequences on the interactive and online advertising industry.

Given the dramatic advances in combating spyware and the guidance now available from enforcement and self-regulatory initiatives that did not exist at the outset of the last Congress, we believe that certain provisions of the bill should be reexamined. I am beginning to believe that certain provisions of the bill would have the effect of stifling innovation among legitimate companies without providing countervailing

consumer benefits in light of such advances. Extreme measures such as prescriptive notice and consent regimes were important two years ago given the pervasiveness of malicious spyware and the lack of clear guidelines for downloadable software. Given the advances described earlier, such regulatory restrictions may no longer be warranted.

Section 3 in particular, could have adverse consequences for legitimate interactive and online advertising. Indeed, as all media advertising increasingly migrates to interactive platforms, we are concerned that this bill may unnecessarily limit businesses interaction with consumers.

We are concerned that the types of software and technologies that would be included under the definition of "information collection program" and the requirements in Section 3 would impact legitimate Internet advertising practices. First, as I have already stated, regulators such as the FTC and state attorneys general, as well as self-regulatory bodies such as TRUSTe, have given clear guidance on the issues addressed in Section 3. Moreover, the bill's broad definitions of "computer software" and "personally identifiable information," as well as its requirements in connection with collection of both "personally identifiable information" and "non-personally identifiable information" tied to advertising extend far beyond addressing the abusive practices that were the impetus for this legislation.

In addition, I am concerned that Section 3 could result in little or no advertising on Web sites that are heavily dependent on advertising that would be regulated by the bill. This, in turn, could limit consumers' rich Internet experiences, innovation, and novel services that are emerging. It could also have the unintended consequence of decreasing the abundance of free content that is currently available to consumers. In addition, it could severely limit a business's ability to accurately describe what it is offering, instead putting all software downloads in the same basket, with the same prescribed disclosure language. Defining software in legislation has proven elusive, and for good reason. Technology advances at an astonishing rate. No one here wants legislation that will limit the use of the cookies, java, html, and Web beacons of the future.

For these reasons, we recommend that the Subcommittee focus on the specific harmful acts, as it did in Section 2, or focus on software that collects truly sensitive information. By targeting a narrower set of actions, legitimate advertisers could continue to deploy innovative technologies, spurring continued Internet growth.

Additionally, IAB member companies share the Subcommittee's goal of ensuring that anti-spyware providers can continue to remove bad software. While we believe that such companies are already succeeding in doing so, we respectfully recognize the goal that the "Good Samaritan" provision contained in Section 5 attempts to achieve. We would, however, have concerns with changes that broaden this language and create a more extensive immunity provision that would afford companies broad discretion to remove legitimate software, which often is misidentified as spyware. Such removals may cause programs to function improperly or not at all. The bill should not include any provision that could result in the unfettered ability of a software company to remove legitimate software without consequence. Such regulation of an emerging technology would preclude major advances as convergence emerges. Ultimately, it would be the consumer who is disadvantaged by this type of provision.

I would like to address several final points that bear mentioning. First, it seems to me that the damages provision extends beyond the consumer protection legislation passed through this Committee and Congress over the years. Second, we should make certain that the preemption provision serves its intended effect of creating a single standard for consumers and businesses. Third, the provision addressing how civil penalties should be determined should simply refer to the section of the FTC Act that addresses this point directly so as not to create confusion among businesses, the FTC, and the courts. Finally, given the rapid changes in technology, we support the sunset provision in the legislation.

Thank you for considering the views of TACODA and 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 continuing to work with you on this legislation.

Mr. RUSH. Thank you, Mr. Morgan.

Our next witness is Ms. Fran Maier. Ms. Maier is the executive director of TRUSTe. TRUSTe is an independent, nonprofit organization that helps consumers and businesses identify trustworthy online organizations through its Web privacy seal. The organization is very supportive of H.R. 964, which establishes many of the same requirements included in TRUSTe's Trusted Download Program.

Ms. Maier, you are recognized for 5 minutes.

STATEMENT OF FRAN MAIER, EXECUTIVE DIRECTOR, TRUSTe

Ms. MAIER. Chairman Rush and Ranking Member Stearns and members of the subcommittee, I am Fran Maier, executive director and president of TRUSTe. We are, as you said, an independent, nonprofit organization and our mission is to advance privacy and trust for a networked world. We do this by serving as a trust authority, bringing together stakeholders and developing programs and best practices. Throughout programs, we aim to recognize and reward, elevate better industry players, responsible industry players.

I want to thank you for the opportunity to speak to the committee about industry self-regulation and our insights on H.R. 964.

First, I would like to talk a little bit about the Trusted Download Program. We have been working on this almost as long as you have been working on this bill for over a couple of years because spyware and unwanted software has really eroded consumer trust in the Internet. We developed the Trusted Download Program with a broad range of stakeholders including our founding partners, AOL, CNET Networks, Computer Associations, Microsoft, Verizon, Yahoo, and the Center for Democracy and Technology. Our program certifies that applications meet requirements for consent, uninstall and affiliate control as well as a number of other rigorous requirements. It is designed to bring accountability and transparency to the downloadable consumer market by creating market incentives for responsible best practices. Our program requirements are rigorous and have been shared with the committee. I would like to add that our certification program includes complete evaluation and monitoring and we use an outside testing lab to make sure that the benefits of certification only go to responsible players.

Interestingly, I think our program requirements are tiered to take into account the many variations in software applications and distribution, so the greater the potential harm to a consumer, the stricter the standards for certification. For example, providers of advertising and tracking software in our program must take full responsibility for how their software is promoted and distributed. This includes the methods used by affiliates, distributors and bundling partners. The first group of nine certified applications were announced on our Whitelist on our Web site last month. We are happy to report that we think that the Trusted Download Program has already had a big impact for the consumer's benefit. One hundred percent of the companies' applications that were certified last month made changes, significant changes to their disclosure or to some of their activities. We have seen that publishers are reducing the size of their affiliate networks in response to the program and

the press that they have received. CNET's *download.com*, which is a portal where consumers download software, is indicating when one of our certified applications is certified so that consumers can make that choice when they decide to download some software, and AOL and Yahoo among others are using the program to make some decisions about who they will partner with and advertise with. We believe to improve consumers' experience, we need both the stick of effective regulation against the bad actors as well as the carrot of market incentives to motivate more responsible players.

Now, to H.R. 964, the Spyware Act. TRUSTe applauds the committee's work on the proposed legislation and you should know that your work has informed the development of the program. Baseline protections for consumers from spyware together with private sector self-regulatory initiatives such as we have will provide tangible relief to consumers. Section 2, which outlines egregious software behavior, and section 3, requirements for notice, consent and uninstall, are very similar to the Trusted Download Program. However, we believe H.R. 964's effectiveness would be strengthened and its impact magnified by inclusion of a safe harbor for self-regulatory compliance programs modeled on the safe harbor provision of the Children's Online Privacy Protection Act. As part of the Safe Harbor, we would want participation in a self-regulatory program as a factor for the court to consider when determining penalties under section 4. A strong safe harbor would further incent companies to implement best practices. We believe that self-regulatory can complement legislation by going beyond legal requirements, respond quickly to consumer concerns and evolve at the fast pace of industry.

I would like to conclude by saying that now that the Trusted Download Program has been launched, there are no more excuses. Advertisers can't say they can't control how their advertising is presented to consumers. Publishers should know whether their software is lacking adequate consumer controls and consent and companies should be able to maintain now that they can see the good software from the bad.

Thank you for this opportunity. We respectfully request that you include a safe harbor to encourage adherence to best practices.

[The prepared statement of Ms. Maier follows:]

PREPARED STATEMENT OF FRAN MAIER
EXECUTIVE DIRECTOR AND PRESIDENT OF TRUSTe
before the
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
ENERGY AND COMMERCE COMMITTEE
U. S. HOUSE OF REPRESENTATIVES
on
H.R. 964 (THE SPY ACT) AND SELF-REGULATION FOR
BEST PRACTICES IN CONSUMER SOFTWARE

MARCH 15, 2007

Chairman Rush, Ranking Member Stearns, and members of the Subcommittee, I am Fran Maier, Executive Director and President of TRUSTe. We are an independent, nonprofit organization with the mission of advancing privacy and trust for a networked world. Through long-term supportive relationships with our licensees, extensive interactions with consumers in our Watchdog Dispute Resolution program, and with the support and guidance of many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosures, informed user consent, and consumer education. I know that many of you are very familiar with our programs, and I am pleased that you have asked me to inform the Committee about private-sector initiatives in downloadable consumer software that have taken place since the Committee last considered the legislation that is now H.R. 964 (The Spy Act). I thank you for the opportunity to tell you about TRUSTe's Trusted Download Program, and to provide our insights on the bill.

H.R. 964 (The Spy Act)

TRUSTe applauds the Committee's work on the proposed legislation to date. We have long articulated a public policy for privacy protection that incorporates the strength of government oversight, the discipline of industry self-governance, and the innovation of privacy-enhancing technology. We are very supportive of a federal law to provide baseline protections for consumers from spyware because such a law, coupled with private sector initiatives to encourage and maintain best practices for downloadable software, will provide tangible relief for Internet users who are currently plagued by problems associated with spyware and unwanted consumer advertising and tracking software.

We applaud section 2 of the bill which outlaws certain egregious activities which should never be employed. We are pleased to note that section 3 of the bill, including the notice and consent and uninstallation requirements are similar to the requirements contained in the TRUSTe Trusted Download Certification Beta Program Requirements, which are attached to this testimony. This should not be a surprise since we used the past work of this Committee in H.R. 29 in the 108th Congress and H.R. 2929 in the 109th Congress as a starting point for the development of our program. From that starting point, we developed additional requirements which I will describe in more detail later in this testimony.

Based on our in-depth work in the consumer software field, we suggest that the effectiveness of H.R. 964 would be strengthened by the inclusion of a safe harbor for industry self-regulatory compliance programs. The primary challenge in legislating online consumer protection practices is ensuring that businesses view the law as a baseline of acceptable practices. The law must provide a floor of protection, not a ceiling.

Legislative safe harbors encourage a flexible self-regulatory regime that, if adhered to, will place a company in compliance with the regulation and create incentives for participation in programs that may exceed protections required by the law. Self-regulatory programs serve as an important first line of defense, responding quickly to consumer complaints, providing ongoing enforcement, and sending the industry a strong message about appropriate practices. They can also adapt to new technologies and business models to continue to protect consumers in light of the ever-changing landscape of on-line threats. Self-regulation elevates good industry actors by certifying them to best practices, and frees government to pick up where voluntary self-governing bodies leave off. Government can focus on bad actors that are not likely to adhere to self-regulation.

Given the global and dynamic nature of the Internet, and the data-gathering technologies that this legislation seeks to address, neither self-regulation nor government oversight can succeed alone. No government agency has the resources to effectively police the Internet without the active support of strong, effective self-governing bodies. Drawing on self-regulation and government oversight together through the framework of a safe harbor, an extremely effective means of both protecting consumers and enhancing e-commerce can be established.

We suggest that such a safe harbor provision be modeled on the provision contained in the Children's Online Privacy Protection Act (COPPA), 15 USC Chapter 9, sec. 1304. COPPA includes a provision enabling industry groups or others to submit for Federal Trade Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. It requires the Commission to act on a request for "safe harbor" treatment, within 180 days of the filing of the request, and after the proposed guidelines have been subject to notice and comment. Section 312.10 of the Children's Online Privacy Protection Rule sets out the criteria

for approval of guidelines and the materials that must be submitted as part of a safe harbor application. As the Federal Trade Commission noted in its February 2007 report to Congress on COPPA implementation, the industry safe harbors approved under COPPA, including TRUSTe's COPPA Safe Harbor Seal Program, have been a success, benefiting consumers and businesses, as well as aiding the Commission in its enforcement efforts.[1]

In addition, we suggest that incentives for participation in industry self-regulatory programs be created by including such participation as a factor that the court shall consider in determining penalties under section 4 of the bill.

The Trusted Download Program Beta

The Trusted Download Program ("the Program"), which we developed with our partners - AOL, CNET Networks, Computer Associates, Microsoft, Verizon, and Yahoo!, and with input from the Center for Democracy and Technology, is the result of more than eighteen months spent in understanding the consumer software marketplace and developing rigorous yet workable certification criteria for consumer downloadable applications. The Program focuses on all consumer software, including advertising and tracking software that may be downloaded to consumers' computers.[2] The Program certifies software applications around Program Requirements which set the industry standard for consumer downloadable software.[3] We are proud to have announced the first group of certified software applications on the Trusted Download Program whitelist on February 16, 2007.[4] Further we are continuing to consult with

[1] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* (February 2007) at 22-24.
[2] The Program does not cover software that is downloaded exclusively to handheld devices, such as cell phones.
[3] The Program Requirements are available as Schedule A to the Trusted Download Beta Certification Agreement (http://truste.org/pdf/Trusted_Download_Beta_Certification_Agreement.pdf).

[4] The White List is available at http://www.truste.org/pvr.php?page=td_licensees.

industry experts, Program participants, advocacy groups and others, to refine our certification processes, standards, testing protocols and business model.

We developed the Trusted Download Program to address a serious problem: the downloading and installation of consumer software without notice or consent. Consumers are understandably frustrated when they discover unexpected software on their computers. In some instances the software application provides real value; in many instances, however, the software may be considered "spyware." A lack of standards and definitions has made it difficult for consumers and businesses alike to distinguish between consumer software programs that utilize intrusive practices that are harmful to consumers, on the one hand, and legitimate software programs that advertise or use information for consumer benefit, on the other. As a result, the promise of easy-to-use and valuable consumer downloadable software has been severely hindered by a lack of trust.

Having recognized the problem and the need for industry action to identify a solution, TRUSTe, together with our partners, worked to build a marketplace for legitimate consumer software by achieving the following objectives:

- To significantly improve the consumer experience with downloadable applications
- To establish the first industry-wide standards for developers of downloadable applications
- To identify and elevate trustworthy applications for distributors and marketers
- To protect the valued brands of online advertisers by enabling them to know which applications are trustworthy and which are not
- Through partners, and potentially through a seal, consumers will also be able to recognize and reward trusted downloads

The Trusted Download Program meets these objectives with a combination of strict standards, thorough review by TRUSTe and by independent, third-party software testing laboratory, ongoing monitoring and enforcement by TRUSTe, and powerful market incentives.

Now I'd like to take a few moments to describe key provisions of the Program Requirements. As I mentioned earlier, many are consistent with H.R. 964; several go beyond the bill's requirements. I would like to make clear that we are not suggesting that the Committee adopt our more restrictive policies, but rather respectfully suggest that it is appropriate for Congress to create incentives for participation in self-regulatory programs that go beyond legal baseline requirements.

The Program Requirements are tiered, to take into account the many variations in software applications; the greater the potential for intrusiveness and harm to consumers, the stricter the standard for certification.

Notice

The Program imposes a layered approach that includes both a "primary notice" when an application is offered, and an easily accessible "reference notice" such as an End User License Agreement (EULA) or a privacy statement. The primary notice, which must present the underlying reason the software company will profit from the download of the application in clear terms, must be provided before consumers can install software. Further, such notice must explain material functionalities that impact the consumer experience, and the notice must be unavoidable. The reference notice supplements the primary notice with additional detailed information, but is not in itself sufficient for providing notice or obtaining consent. In addition,

all advertisements delivered in Trusted Download-certified advertising software must be labeled to identify the software that delivers them.

Consent

All software applications must offer consumers an opportunity to consent to the software download, after receiving the primary notice and prior to installation. This notice must be in plain language and prominently displayed. Consent for downloading advertising and tracking software, in particular, must be obtained through an affirmative act by the consumer (the consent option cannot be the default), and the option not to download software must be of equal prominence. When software is downloaded in a bundle format, where multiple applications are presented after a single download action, each application must present itself separately to the consumer and obtain separate consent.

Easy Removal

Instructions for uninstalling software must be easy to find and understand. Uninstall mechanisms must be available in places where consumers are accustomed to finding them, for example, in the operating system's Add/Remove Programs function. Uninstallation must effectively remove the application from the consumer's computer and the application must not reinstall itself without obtaining new consent. Uninstallation cannot be contingent upon a consumer's providing personally identifiable information, unless that information is required for account verification.

Pseudonymous Information

In addition to requirements governing the collection and use of "personally identifiable information," the Program covers the collection and use of "pseudonymous" information, such as IP addresses, machine IDs, or Web page views, that correspond to a profile or account but is not sufficient, either alone or in combination with easily accessible public information, to identify or contact the individual to whom this information pertains. The inclusion of pseudonymous information within the scope of addressable tracking behavior preserves the program's standards for prior notice and consent for an emerging set of ad serving and tracking applications that track user behavior on the internet and use this information to establish deep profiles or deliver potentially unwanted advertising, all without the collection of personally identifiable information.

Affiliate Controls

One flaw in the current advertising software business model has been the inability (or unwillingness) of the software companies to control the distribution of their software through third parties, where there is often a breakdown in consent to install and easy uninstallation of the software. The Program directly addresses this market failure, and builds on the baseline protections that would be established by H.R. 964, by requiring companies that develop and publish advertising software or tracking software to demonstrate control over their affiliate and distribution networks in order to be certified. Applicants in these markets must provide TRUSTe with complete transparency into their distribution practices, including the financial model, contracted intermediaries, and the end affiliates and bundling partners responsible for promoting their software to consumers. The Federal Trade Commission's recent settlement with Zango,

Inc., imposes a similar requirement, as well as other operational steps that are substantially similar to the Trusted Download Program Requirements.[5]

Prohibited Activities

A software application submitted to the Trusted Download program will not be certified if it, *or any other application owned by the company submitting it*, exhibits behavior that is listed in the Program Requirements as a Prohibited Activity. The list of Prohibited Activities substantially parallels activities prohibited under H.R. 964, and will likely expand in reaction to future developments in the marketplace.

Provisional Certification

The Program requires provisional certification for companies that have engaged in Prohibited Activities in the recent past and for advertising and tracking applications that did not obtain their existing users with proper notice and consent. In order to be fully certified, these companies will be subject to additional oversight, including enhanced monitoring, and a requirement to go back to all consumers who downloaded an uncertified version of their software and obtain their consent for the certified version.

Segregated Advertising Inventory

Advertising software providers whose applications have been certified must maintain segregated advertising inventory, so they can serve advertisements only to consumers whose consent has been obtained in accordance with the Program Requirements.

[5] The Settlement is available on the Commission's Web site at http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf

Monitoring

Certified applications will be monitored by TRUSTe, as well as an independent testing laboratory, for ongoing compliance. The monitoring process includes reviews of primary notice, matching of files to ensure the application has not changed, sampling the affiliate network to verify the integrity of the consumer consent path, and numerous other policy and technology reviews. Pro-active monitoring events are triggered at several points throughout the year for every application in the program. A company risks termination from the Program if TRUSTe verifies a violation of the Program Requirements for any one of its certified software applications.

Enforcement

If monitoring uncovers suspected non-compliance, the software in question, and in certain circumstances all of a company's certified applications, will be subjected to an investigation by TRUSTe. TRUSTe will also open an investigation based on credible evidence of any non-compliance provided by consumers, competitors, or other independent observers. Depending upon the severity of the violation, a company may be suspended from the Program (with a notation to that effect in its listing on the whitelist), or its software application may be removed from the Trusted Download whitelist altogether, or a company may be terminated from the Program and the fact of its termination made public. For the most severe violations, referral to the FTC is also an option.

I'd like to return for a moment to the market incentives inherent in the Trusted Download Program that we believe are its greatest strength and its greatest benefit for consumers and for businesses. As I mentioned earlier, the initial whitelist of Trusted Download certified software

applications is now on our Web site. We expect that consumer portals, advertisers, distributors and other businesses will use the whitelist to decide which software applications to use for advertising or to provide services to consumers. We are already seeing the market react. CNET's Download.com, a leading consumer download portal, is recognizing whitelisted companies on its download assessment page, where consumers decide whether or not to proceed with installation. AOL and others are beginning to extend distribution deals to applications on our whitelist. The Program Requirements, which are also publicly available on our Web site, give guidance to developers of downloadable software on how to build reputable applications that address the requirements of the market regarding notice, consent, and removal. The Requirements increase incentives for software designers to develop trusted applications by giving their potential business partners and advertisers transparency into their practices. Not only must application providers ensure that all new installations are performed with robust notice and consent, but when offering advertising they must additionally separate their user-base into two categories; 1) those obtained with certifiable notice and consent practices, and 2) those obtained prior to the implementation of certifiable notice and consent practices. Providing advertisers with the option to choose audiences will drive up the price of the certified portion, thereby providing the market incentive for application providers to obtain certification and to maximize the portion of their database obtained with best practices. Consumers will reap the benefits of certified downloadable applications, in the form of prominent, understandable disclosures, more explicit mechanisms for controlling software on their computers, easier and effective means of uninstalling that software, and more respectful use of their personal information.

The Trusted Download Program is an excellent example of what industry can accomplish to address consumer protection issues such as those posed by intrusive software downloaded without knowledge or consent of the consumer. With the right mix of leadership, expertise in relevant markets, stakeholder involvement, creativity and a commitment to do the right thing, self-regulatory programs can do credit to industry, complement regulatory initiatives, and benefit consumers and businesses alike. We are proud of the collegial effort that led to the Trusted Download Program, and we're excited to watch as the Program takes off and certified consumer software begins to proliferate.

Conclusion

TRUSTe welcomes this opportunity to share our thoughts on H.R. 964, and to make the Committee aware of our efforts, together with our partners in the Trusted Download Program, to serve as the model for industry best practices in downloadable consumer software. We look forward to working with the Committee, as you continue your own efforts to protect consumers and encourage innovation in the twenty-first century electronic marketplace.

About TRUSTe

TRUSTe was founded in 1997 to act as an independent, unbiased trust entity, and we have earned our reputation as the leading builder of trusting relationships between companies and consumers. The TRUSTe privacy program – based on a branded online seal, the TRUSTe "trustmark" – bridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards. In May 2001, the Federal Trade Commission approved TRUSTe's Children's Privacy Seal Program as a safe harbor under the Children's Online Privacy Protection Act. We are proud to have received that designation. Hundreds of

thousands of young children who are active online are protected by our program, which currently includes some of the most popular Web sites, including www.disney.go.com, and www.kids.msn.com. TRUSTe is also certified as a safe harbor program under the Safe Harbor Framework administered by the U.S. Department of Commerce for U.S. companies wishing to receive personal data from countries in the European Union ("EU"). Our EU Safe Harbor Seal Program gives companies assurance that they are in compliance with the Framework and, therefore, with national data protection laws in all EU member states.

In addition to these efforts, TRUSTe is deeply involved in fostering best practices for email. Our permission-based Email Privacy Seal Program, which allows companies who agree to our strict standards to post a TRUSTe "We Don't Spam" seal on online and offline forms where they collect email addresses, sets the industry standard for best practices consumer email. Finally, we are a California company, and we closely follow developments in California law, to keep our licensees informed about compliance issues. We also work closely with the California Office of Privacy Protection in its ongoing efforts to provide guidance to businesses and consumers on privacy and security issues.

TRUSTe Make Privacy Your Choice

TRUSTe TRUSTED DOWNLOAD CERTIFICATION PROGRAM – BETA PROGRAM REQUIREMENTS

1. DEFINITIONS

(a) Action – means any allegation, investigation, demand, suit, legal proceeding, inquiry, or other legal action, whether formal or informal, initiated by any state or federal governmental authority.

(b) Ad Targeting – The term "Ad Targeting" means the use of Pseudonymous Information to determine User characteristics or preferences for use in ad delivery.

(c) Affiliate – means a person who, for financial consideration, offers the Program Participant's Certified Software to Users in connection with an Affiliate Distribution Program.

(d) Affiliate, High Control – means an Affiliate that, for financial consideration, under a cost per acquisition (pay per install) model with Participant's codes on their site, drives web traffic to Participant's website in order to offer Participant's Software Unit to Users. This distribution method allows the Participant to retain control of the download and installation process for its Certified Software.

(e) Affiliate, Medium Control – means an Affiliate that (1) offers Participant's Software Unit to Users for financial consideration, and (2) in which the Participant controls the download and install process for its Software Unit; typically via some means of centralized software distribution from web servers owned or controlled by the Participant. This distribution method allows the Program Participant to ensure that the correct version of its Software Unit, with all the required disclosures, is downloaded as part of the software bundle distributed by the Affiliate.

(f) Affiliate Distribution Program – means a process whereby (1) a Participant provides financial consideration to one or more Affiliates in exchange for the Affiliate(s)'agreement to offer Certified Software to Users. Typically but not always, as part of the process, at least some Affiliates have the Participant's authorization to hire or subcontract with others to distribute the Participant's Covered Advertising Software or Covered Tracking Software to Users.

(g) Agent – means a third party contracted with to perform a business process, provide a service, or deliver a product on behalf of the principal who retained the agent. An agent does not have an independent right to use the relevant User data on its own behalf or in any way other than to perform its obligations on behalf of the principal. Agents include Service Providers meeting these restrictions.

(h) Anonymous Information– The term "Anonymous Information" means information that does not fall within the definition of either Personally Identifiable Information or Pseudonymous Information . "Anonymous information" includes but is not limited to aggregate information.

(i) Applicant – means a company that has submitted Software for Certification to the Program.

(j) Certification – means the determination by TRUSTe that software submitted to the Program is compliant with the Program Requirements. While Certification applies to software (*i.e.*, the Program does not offer Certification to companies), no company that violates

any company-level Program Requirement (such as performing the Prohibited Activities in Section 12) will be eligible for Certification of any of its software.

(k) Certified Ad Inventory – means the segregated ad inventory that may be displayed only to Users of Covered Advertising Software installed after its Provisional Certification Date or Legacy Users of Covered Advertising Software that was installed prior to the Provisional Certification Date who have received the notice and/or given the consent required under Section 11.

(l) Certified Covered Advertising Software – means a Participant's Covered Advertising Software that has been tested and awarded Certification, and is currently certified under this Program.

(m) Certified Software – means a Participant's Software Unit that has been tested and awarded Certification, including Provisional Certification, and is currently certified under this Program. Certified Software includes, but is not limited to, Certified Covered Advertising Software and Certified Covered Tracking Software.

(n) Certified Covered Tracking Software – means a Program Participant's Covered Tracking Software that has been tested and awarded Certification, and is currently certified under this Program.

(o) Children's Website – means (as defined in Section 312.2 of the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312) a website that, based upon its subject matter, visual or audio content, age of models and other language or characteristics, is targeted or directed to children under the age of thirteen.

(p) Compliance Monitoring – means TRUSTe's monitoring of ongoing compliance with these Program Requirements.

(q) Covered Advertising Software – means software that displays advertisements such that the display of any advertisement is not directly triggered by the User's interaction with the Certified Software, unless such ads are displayed within the context of the application and the use of any other application is not disrupted. TRUSTe may consider other related formats or methods of delivery as part of the scope of the Program. The User's option to disable display of advertising does not exempt software from this definition. Covered Advertising Software is often bundled with other software, such as screensavers, games, weather applications, and other popular User software. Covered Advertising Software may include Covered Tracking Software where the Covered Advertising Software also meets the definition of Covered Tracking Software.

(r) Covered Tracking Software- means any software that collects a User's web browsing or other information entered into a separate application, where a purpose is to transfer such information to a destination off the User's computer that is not controlled by the User. Covered Tracking Software does not include software where the collection and transfer purposes are network integrity or functionality, application integrity, or information security. (Covered Tracking Software may include Covered Advertising Software where the Covered Tracking Software also meets the definition of Covered Advertising Software.)

(s) Default Option – means an option that is pre-selected, so that a User can accept the option without taking any additional affirmative action indicating consent. For purposes of this definition, allowing Users to accept an option by selecting the "Enter" key on their computer keyboards is not an affirmative action indicating affirmative consent.

(t) Distribution Bundle, High Control - means two or more software programs, including Participant's Software Unit and other software, which are offered contemporaneously

to Users by a Distribution Partner, in which the Participant controls the download and install process for its Software, typically by means of centralized software distribution from web servers owned or controlled by the Program Participant. This distribution method allows the Participant to ensure that the correct version of its Software Unit, with all the required disclosures, is consistently downloaded as part of the Distribution Bundle.

(u) Distribution Bundle, Medium Control - means two or more software programs, including Participant's Software Unit and other software, which are offered contemporaneously to Users by a Distribution Partner, in which the Participant does not directly control the download and install process for its Software Unit.

(v) Distribution Partner - means a person that, for financial consideration, distributes Software to Users on behalf of the Program Participant. Typically, but not always, the Distribution Partner includes their own software and/or software from third parties as part of a Distribution Bundle offered to Users.

(w) Effective Date – means the date this Agreement is signed by both parties, or, in the case of a Renewal, the day after the previous license expires, if the requirements for Renewal are satisfied.

(x) EULA – means an End User License Agreement.

(y) Informed Third Party(ies) – means those entities that Participant has designated in writing to TRUSTe to receive Certification status updates, including: failure to obtain Certification, Certification of the Software, placement on the Whitelist, placement on Probation or Suspension status, removal from the Whitelist, and/or termination from the Program.

(z) Just in Time Notice –means notice of a functionality that is added after a User has already consented to install Software but just prior to the execution of that functionality. When this happens, a User is provided with Primary Notice of the new functionality and given the opportunity to provide consent just prior to execution of that functionality. Waiting until just prior to execution of certain functionalities can provide the User with better context to make certain consent decisions. While the Program permits the use of Just in Time Notice for some Certified Software, the Program does not permit its use for Certified Covered Advertising Software. (**Beta Note**: Just in Time Notice may not be used where such use would negatively impact the original value proposition of the Certified Software, as determined by TRUSTe.)

(aa) Legacy User – means all Users who have installed a Participant's Covered Advertising Software or Covered Tracking Software before the Provisional Certification Date of such Covered Advertising Software or Covered Tracking Software.

(bb) Market Research – The term "Market Research" means the use of Pseudonymous Information to understand how Users are using their computers and the Internet.

(cc) Material Change(s) – means an adverse change in a user's rights or protections, that would be of importance or consequence to the User, which may include:

(i) Changes to privacy practices, meaning changes relating to:

(1) Practices regarding notice, disclosure, and use of Personally Identifiable Information and/or Third Party Personally Identifiable Information,

(2) Practices regarding user choice and consent to how Personally Identifiable Information and/or Third Party Personally Identifiable Information is used and shared, or

(3) Measures for data security, integrity, or access.

(ii) Modifications to Certified Software that are relevant to these Program Requirements, including but not limited to:

(1) Changes to one or more functionalities that are required to be disclosed per Sections 3, 5, 6, 7, 10 and 11 of these Program Requirements, and/or;

(2) Changes to the way any required functionalities are disclosed, including but not limited to changes to wording, font, size and/or order of the disclosures, and/or;

(3) Changes to the Software's method or means of storing data remotely.

(iii) Material update or revision to Certified Software functionality including but not limited to: Substantive additions, reconfigurations and/or changes to Software functionality;

(iv) Material Changes do not include any changes which solely affect the performance or integrity of the Software Unit, such as increases in speed, reliability, or information security.

(dd) Non-Certified Ad Inventory – means the segregated ad inventory that is displayed to Legacy Users of Covered Advertising Software that have not received the notice and/or given the consent required under Section 11.

(ee) Notice(s) – means the Primary Notice and the Reference Notice, together and individually.

(ff) Online Preference Marketing (or OPM) – means a process whereby data are typically collected over time and across web pages to determine or predict User characteristics or preferences for use in ad delivery on the web. The OPM process can use Pseudonymous Information or a combination of Personally Identifiable Information and Pseudonymous Information. OPM does not refer to the use of data by Participants for Ad Delivery or Reporting.

(gg) Personally Identifiable Information (or PII) – means any information (i) that identifies or is used to identify, contact, or locate the person to whom such information pertains or (ii) from which identification or contact information of an individual person is derived. Personally Identifiable Information includes, but is not limited to: name, address, phone number, fax number, email address, financial profiles, medical profile, social security number, and credit card information. Additionally, to the extent unique information (which by itself is not Personally Identifiable Information) such as, but not necessarily limited to, a personal profile, unique identifier, biometric information, and/or IP address is associated with Personally Identifiable Information, then such unique information also will be considered Personally Identifiable Information. Notwithstanding the above, Personally Identifiable Information does not include information that is collected anonymously (*i.e.*, without identification of the individual user) or demographic information not connected to an identified individual. Personally Identifiable Information includes Third-Party Personally Identifiable Information.

(hh) Primary Notice – means information actually presented to each user in a manner that is clear, prominent and unavoidable and designed to catch the User's attention during the installation process, prior to completion of the Software Unit(s) installation. The Primary Notice must be fully visible to a User without additional action on the part of the User, such as having to scroll down the page to reach the beginning of the required disclosures. The purpose of the

Primary Notice is to ensure that important information is disclosed to Users in a way that they will see and understand so that they can make an informed decision about the proposed software value proposition.

(ii) Program – means the TRUSTe Trusted Downloadable Certification Program.

(jj) Participant – means a company that has software that is currently certified or provisionally certified in the Program. A participant must have control over all aspects relevant to Certification of the Certified Software.

(kk) Program Requirements – means the requirements for participation in the Program as specified in this Schedule A, as may be amended from time to time.

(ll) Provisional Certification – means an interim level of Certification of a Participant's Software Unit, during which time the Program Participant will be subject to all requirements that apply to its Certified Software as well as certain additional requirements, including, as relevant, those specified in Section 11(c).

(mm) Provisional Certification Date – means the date on which a Participant's Software Unit receives Provisional Certification pursuant to Section 11.

(nn) Provisionally Certified Software – means Software Unit that has received Provisional Certification.

(oo) Pseudonymous Information – The term "Pseudonymous Information" means information that may correspond to a person, account or profile but is not sufficient, either on its own, or through combination with other easily accessible public information, to identify, contact, or locate the person to whom such information pertains. (Beta Note: Examples include but are not limited to a User's IP address, machine ID, and the web pages a User views.)

(pp) Reference Notice – means information that is easy to locate (*e.g.*, via an easily accessible scroll box or a prominent and clearly labeled link) and easy to read and comprehend. Examples of Reference Notices include Privacy Statements and End User License Agreements (EULAs).

(qq) Registered Program Advertiser – means a company that has registered with TRUSTe pursuant to Section 14.

(rr) Service Provider(s) – means a third party that performs or assists in the performance of a function or activity involving the use or disclosure of Personally Identifiable Information or Third Party Personally Identifiable Information.

(ss) Software Disclosures – means the statements made in the Self-Assessment in regard to the software.

(tt) Software Unit – means the Software described in Exhibit 1 that is to be tested and reviewed for Certification by TRUSTe.

(uu) Third-Party Personally Identifiable Information (or "Third-Party PII") - means Personally Identifiable Information that is collected by a Program Participant from a User other than the User to whom it pertains, or whom it identifies. For the purposes of this definition, the collection of Internet search terms entered by a User is not considered PII.

(vv) TRUSTe Marks – means collectively the registered certification marks and trademarks of TRUSTe.

(ww) User – means an authorized user or owner of a computer on which a Software Unit is downloaded.

(xx) Whitelist – means the list maintained by TRUSTe of all Certified and Provisionally Certified software, and the associated Participants that are currently in the Program.

2. Program Management

(a) Certification. The process of certifying Software for compliance with the Program Requirements shall be as provided for below:

(i) Certification shall apply to an individual Software Unit. Participant shall provide TRUSTe with a description, unique identifier and an archival format for each Software Unit it wishes to certify. Participant shall provide TRUSTe with all documentation, whether in written, electronic, or other appropriate format, reasonably requested by TRUSTe in connection with the Certification process. Such documentation shall include a completed Self-Assessment Form, Attestation Form, and other information about the Software as may be reasonably requested by TRUSTe.

(ii) Once Participant has submitted its application, no Material Change is permitted, without written notice to TRUSTe. Any Material Change may trigger restarting the Certification process at TRUSTe's discretion.

(iii) TRUSTe shall review the Self-Assessment and test the Software Unit for compliance with the Program Requirements. The Software Unit version must remain stable until testing is completed. A Certification decision, and corresponding report or reports summarizing TRUSTe's findings, will be provided to the Participant. If TRUSTe does not certify the Software, Participant shall be permitted 30 days time to remedy the failure and resubmit the Software for Certification, whereupon TRUSTe shall provide a second review and test process, and a second report and Certification decision.

(b) Material Changes. Any Material Change to the Certified Software may trigger the need for recertification of the Software, which may require additional fees as provided for herein. TRUSTe will respond to all requests made by Participants to implement Material Changes within five (5) business days of receipt of notice of the requested Material Change.

(c) Participant Obligations. During the Term hereof, and solely with respect to the Software Units for which it seeks certification, the Participant shall:

(i) Make no Material Change to any features, functions, characteristics, architecture, or coding of the Software, in a manner affecting its compliance with the Program, without 1) notifying TRUSTe in writing or electronically of Participant's intent to do so, and 2) obtaining TRUSTe's written decision as to whether such change triggers a recertification requirement;

(ii) Immediately notify TRUSTe in writing of any Material Change in the Software Unit or in the circumstances or facts that initially served as a basis for Certification, or which are otherwise related to Program compliance;

(iii) Immediately provide notice in writing to TRUSTe of any change in the name of a Software Unit or change in the Participant's name;

(iv) Except to the extent prohibited by law, provide notice to TRUSTe of any private lawsuit or Action against it or the Certified Software by any person, law enforcement, or other governmental entity in any country, related to Participant's activities connected to the Program or to the Program Requirements. Such notice shall be provided within five (5) business days of learning of such private lawsuit or Action;

(v) Cooperate with TRUSTe during TRUSTe's Compliance Monitoring and audit activities; and

(vi) Continually provide updated complaint contact information to TRUSTe.

(d) TRUSTe Obligations. TRUSTe shall within a reasonably prompt period of time:

(i) Test the submitted Software and evaluate the Software and Software Disclosures against the Program Requirements;

(ii) Provide a pass/fail decision, as well as a report, regarding the Software and Software Disclosures, to the Participant;

(iii) Retest and provide a second report, as well as a second pass/fail decision, if necessary; and

(iv) Provide ongoing Compliance Monitoring for Software in the Program, to the extent provided for in these Program Requirements.

(e) Whitelist. TRUSTe may, but is not required to, maintain a list of all current Software and/or Participants that are members of the Program ("Whitelist"). Participant hereby consents to the use of its name and the name of the Certified Software on any Whitelist compiled by TRUSTe during the Term. TRUSTe may also respond to any inquiry regarding whether Participant and/or the Software Unit is a member of the Program.

(f) Dispute Resolution. Participants that are also members of the Truste Web Seal Program must participate in TRUSTe's Watchdog process, as described on the TRUSTe website, to resolve non-frivolous, as defined by TRUSTe, privacy concerns or complaints related to Certified Software raised by Users. If Participant does not respond directly to consumer concerns or complaints in a satisfactory and timely fashion, TRUSTe will act as the liaison between the Participant and the consumer to resolve the issue, including recommending any necessary corrective action. (**Beta Note**: It is anticipated that the Program shall include a dispute resolution program for all Participants, not just those that are Licensees of the TRUSTe Web Seal Program. TRUSTe shall operate a User-facing website that accepts inquiries and complaints from Users. TRUSTe or its designee shall refer all inquiries and complaints from Users to the relevant Participant for the Participant's response within a reasonable time to be specified by TRUSTe or its designee. Inquiries and complaints will also, in appropriate circumstances, trigger additional Compliance Monitoring of the Participant's software.)

(g) Updates to Informed Third Parties. TRUSTe will provide ongoing Certification status updates as necessary to Informed Third Parties, if any.

(h) English Only. All Software for which Participant is seeking Certification hereunder must have all User-facing statements written entirely in the English language. Downloading of the Software must be the same no matter the geographic location of the User.

3. Notice. The Program Requirements adopt a layered-notice approach: Program Participants must disclose, or reasonably ensure disclosure in accordance with Section 3, the most important information as outlined below about their Certified Software (including, in the case of Certified Covered Advertising Software or Certified Covered Tracking Software, the proposed value proposition), clearly and prominently, outside of the Reference Notice, prior to installation, along with a link to the Reference Notice.

(a) **The Primary Notice.** The Primary Notice (which is required when any functionality described in Section 3(a) is present) must appear clearly, prominently and unavoidably, before Users can install the Certified Software. Primary notice may be presented

using Just in Time Notice, except in the case of Certified Covered Advertising Software. This Primary Notice must include the following information:

(i) For all Certified Software:

(1) Whether installing the software, alone or as part of a bundle, may:

A. Redirect the User's Internet searches;

B. Add a toolbar to the User's web browser or modify other functionality of the browser or desktop as determined by TRUSTe;

C. Change the User's home page, default search provider or error page handling or otherwise modify browser settings as determined by TRUSTe;

D. Change the User's default provider, web proxy or other changes to Internet settings as determined by TRUSTe; or

E. Cause known material adverse effects on system performance for typical Users as determined by TRUSTe.

(2) A prominent link to all applicable Reference Notices.

(ii) In addition, for all Certified Covered Advertising Software:

(1) The name of the Program Participant.

(2) The essence of the proposed exchange, including (as applicable):

A. The name or brand of the Certified Covered Advertising Software, and if the Certified Covered Advertising Software is bundled with other software (and if such other software has a separate name or brand), the name or brand of the other software;

B. Whether the Certified Covered Advertising Software will perform collection and transfer of information to a computer not under the User's control for the purpose of Ad Targeting and/or Market Research.

C. That ads will be displayed and a brief indication of the types of ads displayed and when ads will be displayed. As applicable, disclose that the ads will appear only while Users are using software in which the Certified Covered Advertising Software is integrated, while they are online generally, or at other specified times; and

D. If applicable, that the software will display ads with pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons.

(3) A prominent link to all applicable Reference Notices.

(iii) In addition, for all Certified Covered Tracking Software:

(1) The name of the Program Participant.

(2) The essence of the proposed exchange, including (as applicable):

A. The name or brand of the Certified Covered Tracking Software, and if the Certified Covered Tracking Software is integrated into or bundled with other software (and if such other software has a separate name or brand, the name or brand of such other software.);

B. When the collection and transfer of information to a computer not under the User's control for the purposes of Ad Targeting and/or Market Research will occur. As applicable, disclose that the collection and transfer of information to a computer not under the User's control will occur only while Users are using the Certified Covered Tracking Software, while they are online generally, or at other specified times; and

(3) A prominent link to all applicable Reference Notices.

(b) **The Reference Notice.** The Reference Notice must be available by prominent link from the Primary Notice, when the Primary Notice is required. In addition the Reference Notice must include at least the following elements:

(i) For All Certified Software:

(1) All of the information contained in the Primary Notice. It is not necessary to have EULA's and/or Privacy Statements tailored to each means of distribution; and

(2) Instructions on how to uninstall the software, as provided for in Section 7.

(ii) In addition, for all Certified Covered Advertising Software:

(1) A description of the types and frequency of the advertisements displayed by the software;

(2) Information (such as a link) on how to access the Program Participant's website and customer support mechanism;

(3) If the software will display ads with pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons, an explanation of how Users can manage their computers to make sure that children are not served with advertisements from Certified Covered Advertising Software installed by adults; and

(4) If the software will display ads with pornographic advertisements or advertisements for alcohol, tobacco, firearms or other weapons, disclosure that software should be installed only by Users age eighteen (18) and over.

(iii) In addition, for all Certified Covered Tracking Software:

(1) Information (such as a link) on how to access the Participant's website and to the Participant's customer support mechanism; and

4. Consent to Install. Participants must provide Users with a means to give their consent to install the Participant's Certified Software prior to the completion of any such installation. The consent mechanism must meet the following standards:

(a) For all Certified Software:

(i) Users must be given a means to indicate their consent to install the Certified Software after receiving all applicable Primary Notices;

(ii) The language used to describe Users' options to consent to install Certified Software must be plain and direct;

(iii) Installation of software shall not proceed if a User declines consent to install the Certified Software or closes the dialog box containing the consent option; and

(iv) Users may only be asked once in any installation process to reconsider their decision not to install software or to close the dialog box with the consent option, unless Users have indicated it is acceptable to ask them later.

(b) In addition, for all Certified Covered Advertising Software and Certified Covered Tracking Software:

(i) Users must be given a means to indicate their consent to install the software after receiving any applicable Primary Notice, and the option to consent may not be the Default Option; and

(ii) The option to decline consent to install Certified Covered Advertising Software or Certified Covered Tracking Software must be of equal prominence to the option to consent to the installation of Certified Covered Advertising Software or Certified Covered Tracking Software.

5. Notice and Choice Requirements for Uses of PII and Pseudonymous Information.

(a) **Primary Notice.** If PII or Pseudonymous Information is collected and transferred to a computer not under the User's control through the Certified Software, the following information must be provided in a Primary Notice:

(i) For all Certified Software: Either (i) a link to the Reference Notice, or (ii) instructions on where the user can find the Reference Notice, alerting Users to the information about choices available to them regarding their data.

(ii) In addition, for all Certified Covered Advertising Software or Certified Covered Tracking Software: A description of the PII collected or transferred to a computer not under the User's control through the Software Unit, the uses of PII obtained through the Certified Software by Participant, and the types of companies to which Participant will transfer PII.

(**Beta Note**:With TRUSTe's prior approval, certain information required to be included in the Primary Notice may be moved to a "learn more about this" link, as long as all required disclosures are complete, clear, prominent and unavoidable, in TRUSTe's sole judgment and discretion.)

(b) **The Reference Notice.** If PII or Pseudonymous Information is collected through the Certified Software, the Reference Notice must be available by prominent link from the Primary Notice. The Reference Notice must include at least the following elements:

(i) For All Certified Software:

(1) Whether the software collects PII, and if so, the following additional disclosures:

A. What PII is being collected;

B. The identity (including name, address and e-mail address)of the entity collecting such information;

C. How such information will be used;

D. A description of the types of entities with whom the information is shared, if at all;

E. The purposes for which data is disclosed to third parties;

F. How and when the User may exercise choice, as required in Section 5(c), below;

G. Whether Users' PII will be supplemented with information from other sources;

H. The User's access rights to correct material inaccuracies in Personally Identifiable Information, such as account or contact information; and

I. A general statement describing data security practices (Beta Note: Program Participant must implement reasonable procedures to protect Personally Identifiable Information and/or Third Party Personally Identifiable Information within its control from unauthorized use, alteration, disclosure, distribution, or access. Program Participant shall utilize appropriate, commercially reasonable means, such as encryption, to protect any sensitive information, such as social security numbers, financial account and transaction information, and health information that it collects.)

(2) In addition, for all Certified Covered Advertising Software or Certified Covered Tracking Software:

A. Whether the Certified Software collects Pseudonymous Information, and if so, the following additional disclosures:

I. The types of Pseudonymous Information collected by the Certified Software;

II. The Participant's use of Pseudonymous Information;

III. Whether the Participant shares Pseudonymous Information with Third Parties and if so, whether the Program Participant places any restrictions on its further use or dissemination; and

IV. Additionally, the Reference Notice must contain information, such as a link, on how to access the Participant's website and the Participant's customer support mechanism.

(c) **Choice Requirements**.

(i) For All Certified Software:

(1) The User to whom PII pertains must be offered an opt-out choice if PII collected through the software may be used in the following ways:

A. Use not related to the primary purpose for which the User provided it. The scope of use deemed related to the primary purpose shall be defined in the Reference Notice and shall be reasonable to Users;

B. Disclosure or distribution to third parties, other than Agents; or

C. Merger of Pseudonymous Information with previously collected PII on a going forward basis (*i.e.*, after the user provides PII) for use in Online Preference Marketing, where such use had not been previously disclosed to and accepted by the User.

D. Certified Software Providers may require the collection or use of PII as part of the value proposition of the software, and may decline to provide the software if User opts out from such use.

(2) The User to whom PII pertains must be provided with notice and provide his or her affirmative consent prior to the merger of PII with Pseudonymous Information previously collected through the software for use in Online Preference Marketing.

(3) Before Third-Party PII collected through the software may be used or disclosed for any purpose other than the primary purpose for which such information was collected, the person to whom such information pertains must provide affirmative consent. [Notwithstanding such restriction, such information (i) may be disclosed pursuant to legal process (*e.g.*, subpoenas, warrants) or (ii) may be used to send a one-time e-mail message to the person to whom the information pertains in order to solicit such opt-in consent.] [**Beta Note**: One example of the behavior this provision is intended to prohibit is the use of Third-Party PII collected through the software (e.g., via an address book) to send unsolicited bulk communications to third parties.]

6. Special Requirements for Certified Covered Advertising Software. Consumers should be able to understand why they receive ads from a Participant. The mechanism displaying Ads in Certified Covered Advertising Software must be branded so that Users understand the name of the Certified Covered Advertising Software, the name of any software that has bundled with the

Certified Covered Advertising Software, and the name of the Participant providing the Certified Covered Advertising Software.

(a) **Reaffirmation**. Shortly after the User consents to the installation, Certified Covered Advertising Software must display an informational notice that (i) demonstrates a representative example of the Certified Covered Advertising Software's advertisements, (ii) provides the User with more information on how the Covered Advertising Software functions, and (iii) provides information on how to uninstall the software, which may be provided via a prominently labeled link. (**Beta Note**: When a Covered Advertising Software provider has more than one format, a representative example must be sufficient to enable a reasonable User to make an informed decision.)

(b) **Branding.** Advertisements displayed by Certified Covered Advertising Software must be branded with, or within close proximity to, the name of the Participant and the brand of the Certified Covered Advertising Software (if distinct from the name of the Participant).

(c) **Co-Branding. The mechanism displaying the** advertisement must also contain, on their face, or via prominently labeled link, a list of the programs and, if applicable, a representative list of the content that cause the display of such advertisements including clear instructions for removal of the Certified Covered Advertising Software. The link itself must be clearly labeled to communicate to Users that (i) the advertisement was displayed because the User has certain software titles on his computer and, if applicable, access to certain web-based content; and (ii) that the link will take the User to a list of those programs. (**Beta Note**: It is anticipated that this Section 6(c) will be amended, in a time period that is reasonable given the technical challenges, to require that Certified Covered Advertising Software make the list of programs referred to in this sub-section displayable within the advertisement itself and not merely as a link.)

7. Uninstall. Certified Software must provide Users with an easy and intuitive means of uninstallation. In addition, the following uninstall requirements shall also apply.

(a) For all Certified Software:

(i) The name of the Certified Software must be listed in the customary place for user initiated uninstall within the software platform (*e.g.*, an Add/Remove Programs facility in the Windows operating system);

(ii) Uninstallation of Certified Software must remove the Certified Software from the User's computer. Uninstallation of Certified Software may be conditioned on the uninstallation of other software on a User's computer (for example, uninstallation of Certified Covered Advertising Software may be conditioned on the uninstallation of other software that is bundled with the Certified Covered Advertising Software), provided that the other software meets the uninstall requirements of this section; (**Beta Note**: TRUSTe recognizes that Certified Software may require the User to install other software (*e.g.*, Adobe Acrobat, Flash), and that the other software may legitimately remain on a User's computer after uninstallation of the Certified Software. TRUSTe, in its discretion, will determine whether or not the other software is left behind after uninstallation for a legitimate reason; for example, because the User has installed software program(s) that also require the use of the other software in order to function.);

(iii) Once a User has uninstalled Certified Software, the Certified Software may not reinstall on a User's computer unless the reinstallation is performed pursuant to the Program Requirements and, in particular, pursuant to new consent;

(iv) Uninstall instructions for all Certified Software must also be available from the Participant's web page either directly or through a link. (**Beta Note:** TRUSTe

anticipates a future requirement that Certified Software provide a link to the TRUSTe web page where uninstall instructions are posted); and

(v) No PII shall be required in order to uninstall Certified Software unless the PII was previously collected in compliance with the Program, and it is reasonably necessary, and only used, to authenticate and/or identify the User.

(b) In addition, for all Certified Covered Advertising Software:

(i) Uninstallation instructions for Certified Covered Advertising Software must be available in multiple places that are easy for Users to find. At a minimum, uninstall instructions must be available:

(1) By a link from the advertisements themselves, or from the browser window or frame where such content is provided, or from a conspicuous and recognizable icon;

(2) In the Reference Notice;

(3) By link from a listing in the Start/Programs menu (or functionally similar menu in other non-Windows software platforms); and

(4) On the Program Participant's website.

(ii) Customer support information for Users' uninstall questions must be available by link from the software mechanism displaying the advertisements.

(c) In addition, for all Certified Covered Tracking Software:

(i) Uninstallation instructions for Certified Covered Tracking Software must be available in multiple places that are easy for Users to find. At a minimum, uninstall instructions must be available:

(1) In the Reference Notice;

(2) By link from a listing in the Start/Programs menu (or functionally similar menu in other non-Windows software platforms); and

(3) On the Participant's website.

8. Software or Notice Updates.

(a) A Participant cannot retroactively apply Material Changes to the Certified Software or to the Privacy Statement or EULA of Certified Software unless it gives Users Primary Notice of the change and an opportunity to uninstall the Certified Software prior to applying the change. Changes to installed Certified Software that would transform it into Covered Advertising Software or Covered Tracking Software must be treated as a new installation under these Program requirements.

9. Third-Party Distribution / Affiliate Practices.

For all Covered Advertising Software or Covered Tracking Software; and certain Certified Software of Participants, as determined by TRUSTe, who distribute Software Units via Distribution Partners; Affiliates, High Control; or Affiliates, Medium Control;

(a) If Participants use Distribution Partners or Affiliates, they must:

(i) Have contractual provisions in place with such Distribution Partners and Affiliates prohibiting them from causing Participant's Certified Software to not comply with these Program Requirements. In the context of an Affiliate Distribution Program, the contract between the Program Participant and its Affiliate must further require that contracts between the Affiliate and its subcontractors bind the subcontractors to comply with these Program Requirements;

(ii) Disclose to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the names of Distribution Partners and Affiliates as well as locations (e.g. URLs of affiliates within an Affiliate Distribution Program) where such Distribution Partners and Affiliates provide or drive traffic to Certified Software to consumers so that such third-party distribution and affiliate practices may be reviewed, tested, and monitored for compliance with these Program Requirements;

(iii) Disclose to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the modifications that Distribution Partners or Affiliates are permitted to make to Certified Software as well as locations where Distribution Partners and Affiliates provide such modified Certified Software to Users so that such modifications may be monitored for compliance with these Program Requirements;

(iv) Demonstrate to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, that Participant has an effective process for evaluating Distribution Partners and Affiliates within an Affiliate Distribution Program;

(v) Evaluate on an ongoing basis Distribution Partners and Affiliates, and report any known material non-compliance with these Program Requirements involving Certified Software. Failure to report any such substantive non-compliance in a timely manner shall be grounds for a suspension or termination of a Participant from the Program and de-certification of all or any of such Program Participant's Certified Software; and

(vi) If the Program Participant learns that a Distribution Partner or Affiliate has engaged in practices that materially violate these Program Requirements, the Program Participant must follow the Program's specified re-opt-in procedures (as specified in Section 11 of these Program Requirements) to re-opt in at least one User of each computer that may have received the Certified Software by those means.

10. Special Protections for Children. Participants with Certified Covered Advertising Software or Certified Covered Tracking Software must take the following steps:

(a) Prevent the distribution of their Certified Covered Advertising Software or Certified Covered Tracking Software on Children's Websites, including by prohibiting their Distribution Partners and Affiliates from such distribution;

(b) Engage in commercially reasonable oversight to determine where advertisements promoting the installation of their Certified Covered Advertising Software or Certified Covered Tracking Software appear;

(c) If their Certified Covered Advertising Software delivers pornographic advertisements or advertisements for alcohol, tobacco, firearms or other weapons, disclose in the Reference Notice that their Certified Covered Advertising Software or Certified Covered Tracking Software should be installed only by Users age 18 and over;

(d) If their Certified Covered Advertising Software delivers pornographic advertisements or advertisements for alcohol, tobacco, firearms or other weapons, Program

Participants must ensure that such ads are branded so that they may be recognized by child protection software filters by either;

(i) including the phrase "for adults 18 years" in text somewhere on the face of the Covered Advertisement, or

(ii) including the phrase "for adults 18 years" in the meta keyword tag for the page containing the Covered Advertisement, or

(iii) including the phrase "for adults 18 years" within the "alt", "name" or "id" attribute of the image tags within the Covered Advertisement; and

(e) Follow the branding steps in Section 6 to make sure that each time Users of Certified Covered Advertising Software see an advertisement, they have a means of understanding why they received the advertisement and easy-to-find information on how to stop getting advertisements from the Certified Covered Advertising Software.

11. Provisional Certification. In certain cases additional transparency may be useful to companies considering partnerships with Participants. In particular, companies may desire transparency into both (i) the recent, though terminated, prior practices of a potential partner that are prohibited under Section 12 of these Program Requirements; or (ii) the efforts of a Participant to provide Legacy Users of a Participant's Certified Covered Advertising Software or Certified Covered Tracking Software with the level of notice now required under this Program. In order to provide such additional transparency, Program Applicants that would otherwise be entitled to Certification of their Software shall have their Software be eligible only for Provisional Certification in the following circumstances:

(a) Legacy Users of Covered Advertising Software or Covered Tracking Software. Compliance with the Program Requirements for new installations of Covered Advertising Software or Covered Tracking Software is just one step in receiving Certification for such Covered Advertising Software or Covered Tracking Software. The next step is making sure that all Users who previously received such Covered Advertising Software or Covered Tracking Software from the Participant (the "Legacy Users") fully understand the deal they have made and continue to agree to it. To that end, the Program requires a three-step process to achieve full Certification for Covered Advertising Software or Covered Tracking Software.

(i) Step One: Applicant Status. Potential Participants meet the first step, Applicant status, by submitting their software to the Program for review and by obligating themselves to timely make all changes necessary to comply with the Program both prospectively and retroactively as applied to Legacy Users of their Covered Advertising Software or Covered Tracking Software.

(ii) Step Two: Provisional Certification for New Installs and Client Software Upgrades. Once an Applicant has submitted its Covered Advertising Software or Covered Tracking Software to the Program, the Applicant and its software has been determined by TRUSTe to meet the Program Requirements, and the Applicant has warranted that on an ongoing basis all new installations of such Covered Advertising Software or Covered Tracking Software installations will meet the Program Requirements, the submitted Covered Advertising Software or Covered Tracking Software shall receive Provisional Certification ("Provisional Certification Date"). Participants with Provisionally Certified Software that is Covered Advertising Software or Covered Tracking Software shall be required to do the following:

(1) Within six (6) months of the Provisional Certification Date, the Program Participant must initiate updating/upgrading the Covered Advertising Software or Covered Tracking Software

programs of their Legacy Users, where possible, recognizing that some distribution contracts may not allow for Program Participants software to be modified to become a compliant Covered Advertising Software or Covered Tracking Software program. (**Beta Note:** TRUSTe recognizes that some existing contracts may prohibit the required changes; nevertheless, TRUSTe will not fully certify software that has not been updated/upgraded in accordance with this provision.)

(2) Immediately undergo a higher degree of Compliance Monitoring of its Covered Advertising Software or Covered Tracking Software under the Program.

(3) Immediately segregate the advertising inventory that is displayed to its Covered Advertising Software Users into two distinct sets: Certified Ad Inventory and Non-Certified Ad Inventory.

A. Certified Ad Inventory shall be inventory that is displayed to Users of Covered Advertising Software installed after the Provisional Certification Date (and thus compliant with these Program Requirements) or displayed to Legacy Users of Covered Advertising Software that was installed prior to the Provisional Certification Date who have received the notice and/or given the consent required under Section 11(a)(iii) below.

B. Non-Certified Ad Inventory shall be inventory that is displayed to Legacy Users of Covered Advertising Software that who not received the notice and/or given the consent required under Section 11(a)(iii) below.

(4) Explicitly make available to advertisers the ability to purchase only Certified Ad Inventory described in Section 11(a)(ii)(3) above.

(5) Ensure that no advertisements from Registered Program Advertisers (see Section 14 below) appear within Non-Certified Ad Inventory.

(iii) Step Three: Messaging to Legacy Users. Understanding that the Program represents a new, comprehensive standard, and that some Participants have modified their practices over time, the Program allows for a two-tiered notice and consent regime to Legacy Users.

(1) Participants must complete the appropriate form of messaging, as applicable, within nine (9) months of the Provisional Certification Date to achieve full Certified status for their Provisionally Certified Covered Advertising Software or Covered Tracking Software.

A. Legacy Users Who Received Covered Advertising Software or Covered Tracking Software Under Substantially Compliant Disclosures. Legacy Users who received Covered Advertising Software or Covered

Tracking Software pursuant to disclosures substantially similar to those in Sections 3 and 5 and who consented to the installation must be given a notice describing the material facts about the operation of the software including uninstallation instructions.

B. Legacy Users Who Received Covered Advertising Software or Covered Tracking Software Under Disclosures Not Substantially Compliant with These Program Requirements - Legacy Users who received Covered Advertising Software or Covered Tracking Software pursuant to disclosures not substantially similar to those in Sections 3 and 5 must be given a notice describing the material facts about the operation of the software and an opportunity to provide consent to continue to have the Covered Advertising Software or Covered Tracking Software on their systems or to uninstall the Covered Advertising Software or Covered Tracking Software. The option to provide consent may not be the Default Option. Users who decline consent or who close the dialog box shall be promptly provided with uninstall instructions. If the User subsequently fails to uninstall the software, any ads served to that User must be part of the Program Participant's Non-Certified Ad Inventory.

(2) After the full program launch Covered Advertising Software and Covered Tracking Software can no longer serve ads to those Users who have not re-opted in per the Program Requirements.

(b) Other Activities that Trigger Provisional Certification. In TRUSTe's discretion, TRUSTe may designate a Participant's Certified Software as Provisionally Certified if other substantial risk factors calling into question the credibility of the Participant are present, after providing notice to the Participant and a reasonable opportunity to respond.

(c) Additional Requirements for Program Participants with Provisionally Certified Software.

(i) Notwithstanding any written consent obtained pursuant to Section 2(a) of the Agreement, Program Participants with Provisionally Certified Software may not mention their software's Certification in any manner without including the qualification "Provisional."

(ii) Participants with Provisionally Certified Software may be subject to additional Compliance Monitoring or reporting requirements as determined by TRUSTe.

(iii) Provisionally Certified Software will be so designated on a webpage maintained by TRUSTe.

(iv) Provisionally Certified Software will be so designated on any Whitelists maintained by TRUSTe.

(d) Evaluator Requirement - Participants and Program Applicants that meet the following criteria may be required to submit to an evaluation of their compliance with the Program, including Section 11(a)(iii), if applicable.

(i) Evaluation Criteria:

(1) If Program Applicant asserts that one of more of its Legacy Users were acquired in compliance with Program Requirements as per Section 11(a)(iii)(1)(A), TRUSTe may require that they submit to an evaluation of the methods and procedures used in making that determination.

(2) If Program Applicant or Participant currently distributes their Covered Advertising Software or Covered Tracking Software with one or more Medium Control Affiliates, TRUSTe may require that the Program Applicant or Participant submit to an evaluation of the business practices for each of the Program Applicant's or Participant's Affiliates and all Distribution Partners as they reasonably pertain to these Program Requirements.

(3) If Program Applicant or Participant currently is, or within the past six months was, under investigation by Federal Trade Commission, State Attorneys General, or similar body, TRUSTe may require that Program Applicant or Participant submit to an evaluation of all business practices that reasonably pertain to these Program Requirements.

(4) If Program Applicant or Participant is, or becomes, within six month of application to the Program, the subject of a publicly filed proceeding and/or settlement by the Federal Trade Commission, State Attorneys General, or similar body, TRUSTe may require that Program Applicant or Participant submit to an evaluation of all of its business practices that reasonably pertain to these Program Requirements.

(ii) Evaluation Scope

(1) The evaluations are to be performed by, in TRUSTe's discretion, either TRUSTe or a firm chosen by the Program Participant from a list of pre-selected evaluators deemed suitable by TRUSTe, and will occur during normal business hours and at a time mutually agreed to by the Participant and the evaluator.

(2) The results of the evaluation shall be confidential, provided that the top-level results of all evaluations shall be provided to TRUSTe upon completion.

(3) In all instances, TRUSTe reserves the right define the scope of the evaluation.

(iii) Eligibility for Full Certification. Participants with Provisionally Certified Software will be eligible for full Certification of their compliant Software Unit(s) upon the last to occur of the following:

(1) Six (6) months following the Provisional Certification Date;

(2) The provision of top-level evaluation results to TRUSTe that demonstrate compliance with the Program; and

(3) Satisfaction of the requirements described in Section 11, if applicable.

(iv) Notwithstanding any distribution contract constraints, Participants with Legacy Users must re-opt in such Legacy Users within one (1) year.

12. Prohibited Activities. All Participants shall not, and shall take steps in accordance with Section 9 to ensure that their Distribution Partners or Affiliates do not, do any of the following: (**Beta Note**: It is anticipated that additional Prohibited Activities may be added to this list over time.)

(a) Take control of a User's computer by deceptively:

(i) using the computer to send unsolicited information or material from the computer to others;

(ii) accessing, hijacking or otherwise using the computer's modem or Internet connection or service and thereby causing damage to the computer or causing the owner or authorized User, or a third party defrauded by such conduct, to incur charges or other costs for a service that is not authorized by the owner or User;

(iii) using the computer as part of an activity performed by a group of computers that causes damage to another computer;

(iv) delivering advertisements that a User cannot close without turning off the computer or closing all other sessions of the Internet browser for the computer; or

(v) using rootkits or other software that are typically used to hack into a computer and gain administrative-level access for unauthorized use of a computer.

(b) Modify security or other settings of the computer that protect information about the User for the purposes of causing damage or harm to the computer or the User.

(c) Collect PII through the use of a keystroke logging function without authority of the owner of the computer.

(d) Induce the User to provide PII to another person by intentionally misrepresenting the identity of the person seeking the information. This includes inducing the disclosure of information by means of a web page or Software Unit that:

(i) is substantially similar to a web page or Software Unit established or provided by another person; and

(ii) misleads the User that such web page or Software Unit is provided by such other person.

(e) Induce the User to install the Software onto the computer, or prevent reasonable efforts to block the installation or execution of, or to disable the Software, by:

(i) presenting the User with an option to decline installation but, when the option is selected by the User or when the User reasonably attempts to decline the installation, the installation nevertheless proceeds;

(ii) misrepresenting that the Software will be uninstalled or disabled by a User's action, with actual or constructive knowledge that the Software will not be so uninstalled or disabled;

(iii) causing software that the User has properly removed or disabled to automatically reinstall or reactivate on the computer;

(iv) changing or concealing the name, location or other designation information of the software for the purpose of preventing a User from locating the software to remove it;

(v) using randomized or intentionally deceptive file names, directory folders, formats or registry entries for the purpose of avoiding detection and removal by a User;

(vi) causing the installation of software in a particular computer directory or computer memory for the purpose of evading a User's attempt to remove the software;

(vii) requiring completion of a survey, or disclosure of PII, to uninstall software;

(viii) requiring, without the authority of the owner of the computer, that a User obtain a special code or download a third-party program to uninstall the software; or

(ix) intentionally causing damage to or removing any vital component of the operating system when uninstallation is attempted.

(f) Misrepresent that installing software or providing log-in and password information is necessary for security or privacy reasons unrelated to the software itself, or that installing software is necessary to open, view or play a particular type of content online or offline (*e.g.*, can not falsely state software is necessary for accessing web site).

(g) Induce the User to install, download or execute software by misrepresenting the identity or authority of the person or entity providing the software to the User. This includes, but is not limited to use of domains with misspelling of frequently visited web sites (*i.e.*, 404 squatting).

(h) Remove, disable, or render inoperative by deceptive means a security, anti-spyware or anti-virus technology installed on the computer without obtaining prior consent from the User.

(i) Install or execute the Software on the computer with the intent of causing a person to use the software in a way that violates any other provision of this section.

(j) Allow any of their Certified Software to be bundled with the Software unit currently engaging in any of the Prohibited Activities listed in this section.

13. Scope of Certification. Material Changes to the Certified Software may trigger a recertification requirement.

14. Advertiser Registry. TRUSTe shall maintain a website for advertisers to enroll as Registered Program Advertisers.

Mr. RUSH. Thank you, Ms. Maier.

Our next and final witness for this morning's hearing is Ms. Christine A. Varney from the law firm of Hogan and Hartson LLP. She is speaking on behalf of Zango Incorporated. Zango is an online media company that provides consumers with proper online media and programming in exchange for their consent to download adware onto their computers. Previously, as 180 Solutions, the company settled FTC charges that it used unfair and deceptive practices to install unwanted adware that was deliberately difficult to remove. The settlement disgorged Zango of $3 million in ill-gotten gains and presently bars the company from installing any adware software onto a consumer's computer without his or her explicit consent and an easy means of removing it. Zango was lost in the dark and now they see the light. They support H.R. 964 except for section 5(c), the Good Samaritan section, which it believes to be anti-competitive and subject to abuse.

Ms. Varney, you are recognized for 5 minutes for your opening statement.

STATEMENT OF CHRISTINE A. VARNEY, HOGAN & HARTSON LLP, ON BEHALF OF ZANGO, INC.

Ms. VARNEY. Thank you, Mr. Chairman. I was getting a little worried there until you got to the "see the light" part.

Chairman Rush, Ranking Member Stearns and members of the subcommittee, as the chairman said, I am Christine Varney. I am head of the Internet practice at Hogan and Hartson, and in the spirit of full disclosure, I am a founder and past chair and current board member of TRUSTe. I am also a former Federal Trade commissioner.

As the chairman said, I am appearing here today on behalf of my client Zango and Zango appreciates the opportunity to share its support for 964 and join the chorus of support that you are hearing for the bill. Just a moment about Zango and then we will talk just for a few moments about the specific provisions of the bill.

Zango provides consumers with access to a large and expanding catalog of more than 100,000 pieces of Web content including online video, games, music tools and utilities. Much like television, this content is funded by advertising and available to consumers without charge. Twenty million consumers have chosen to enjoy this content and tens of thousands of consumers elect to download Zango software every day. At the same time, this business model offers smaller content providers and Web publishers the opportunity to monetize their creations and their online traffic by delivering to advertisers a receptive consumer when that consumer is most likely to be making an online purchasing decision. The company has more than 3,000 advertising partners. Zango's desktop advertising model differs from other marketing applications in several respects. First and foremost, Zango's pre-download notice and consent process will meet the requirements of H.R. 964 as does its uninstall and labeling features. Second, Zango does not track or collect any user's personally identifiable information. In short, Zango is not spying on anyone. Third, instead of merely providing links in response to a search query or distracting the user with multiple click-throughs, Zango delivers an advertiser's specific Web

page in response to the consumer's search for a related product or service. This gives the consumer the benefit of comparative offers on the Web at the time the consumer is looking to acquire something.

Although, as I have emphasized, Zango is not spyware, the company long ago recognized that its success and ultimately the success of its business model was dependent upon Internet users understanding and trusting its value proposition and upon a level regulatory playing field for all online advertisers. Thus, Zango has supported congressional action in this area since the 108th Congress when it endorsed the bill reported by this committee. As with that bill, H.R. 964's greatest strength is its recognition that conduct and intentions underlying different forms of downloadable software require different approaches.

Zango supports section 2 and 3 of the bill which appropriately and carefully distinguish between software functions that are per se unacceptable versus those for which consumer choice and consumer benefits are preserved with appropriate consumer protection. Zango also commends the authors of the bill for continuing to include the preemption provisions of section 6 and the tracking cookie study in section 8.

We are concerned, however, about subsection 5(c), which has been described as a liability exception for the so-called Good Samaritans. This provision unnecessarily restricts the FTC's ability to pursue enforcement action against those parties the FTC believes warrant it. Equally important, the presence of such an immunity provision in the bill opens the door wide to judicial application and expansion of the concept in private litigation between commercial parties. Some companies selling scanning applications to consumers compete by issuing inflammatory warnings designed to frighten consumers about software lurking on their computers. It will not be long before purported congressional policy protecting Good Samaritans is cited as a legal basis for defending against or dismissing a civil claim brought by a software provider against one of these applications or even a claim brought by one of these applications against another. There is no compelling reason in this instance to alter the standard that commercial disputes between commercial parties should be settled commercially or short of that, in the courts in private litigation. The conduct of commercial parties should not be exempted from the FTC enforcement authority merely due to the alleged nature of the particular product or service being sold. Zango respectfully urges the committee to delete subsection 5(c).

All participants in the online advertising industry should embrace and implement the standards set forth in section 3 of H.R. 964, as Zango has, but unfortunately, not all will. Too many in fact will not until they are compelled to do so. As the desktop advertising industry evolves, Zango will continue to strengthen its business practices and enhance its technology to make the online economy increasingly valuable by enabling consumers, advertisers, publishers and content providers to seamlessly work together. With the one modification suggested, H.R. 964 is fully supported by Zango and we urge its enactment.

I have submitted longer written remarks for the record, and I look forward to your questions.

[The prepared statement of Ms. Varney follows:]

TESTIMONY OF
CHRISTINE A. VARNEY, ESQUIRE
HOGAN & HARTSON LLP
On Behalf of
ZANGO, INC.
Before the
SUBCOMMITTEE ON COMMERCE, TRADE
AND CONSUMER PROTECTION
THURSDAY, MARCH 15, 2007

Chairman Rush, Ranking Member Stearns, and Members of the Subcommittee:

I am Christine Varney, a partner in the law firm of Hogan & Hartson LLP, and I am appearing here today on behalf of my client Zango, Inc., an online media company based in Bellevue, Washington, outside Seattle. Zango appreciates being given the opportunity to share with the Subcommittee its views on H.R. 964, the "Securely Protect Yourself Against Cyber Trespass Act," and I am pleased to be here to represent them.

Zango provides consumers with access to a large and ever-expanding catalog of more than 100,000 pieces of premium Web content, including online videos, games, music, tools, and utilities. Much like television, this content is funded by advertising and can therefore be provided free to consumers. Using a clear and conspicuous notice and consent process, 20 million consumers have chosen to enjoy those benefits, and tens of thousands of consumers elect to download Zango software every day. At the same time, this business model offers content providers and Web publishers the opportunity to monetize their creations and their online traffic. It does so by delivering to advertisers a receptive consumer audience when consumers are most likely to be making an online purchasing decision.

The company has more than 3,000 advertising partners. Advertisers purchase keywords from Zango in a manner similar to purchasing keywords from paid search engine providers like Google or Yahoo. Consumers in turn gain access to the free content by installing Zango's proprietary software, which today is served directly from the company's own servers in order to give the company appropriate control over the notice and consent process described in further detail below. Zango's Web publisher network includes direct relationships with several hundred Internet businesses operating thousands of Web sites. These Web publishers monetize premium portions of their Web sites by requiring users to install Zango in order to access that content without charge. Zango also works with online content providers, delivering them a much-needed revenue stream in order to continue to develop content that can be kept free for consumers.

In short, Zango links the consumer, content provider, Web publisher, and advertiser into one cohesive online ecosystem – in effect, a "Content Economy" that offers each participant a level of access, opportunity, and return never before possible. The company has also won recognition for its achievements from several objective observers of the online industry. This year Zango was named one of AlwaysOn Media's "Top 100 Private Companies," and in 2005 it ranked number 7 on the Inc. 500 "Fastest Growing Private Companies" list. That same year, CEO Keith Smith was named one of Fortune Small Business' "Best Bosses," and in several recent years the company was recognized by Washington CEO Magazine as one Washington State's "Best Companies to Work For".*

* In connection with its acquisition of another firm during the summer of 2006, the company changed its corporate name from 180solutions, Inc. to Zango, Inc., reflecting the brand name of its primary consumer software product. The honors mentioned above prior to mid-2006 were awarded to 180solutions, Inc., but the company's senior management team have remained the same following the acquisition, including its CEO, President and COO, and Executive Vice President and Chief Compliance Officer.

How Zango Works

Zango's desktop advertising model differs from other marketing applications in several respects. First and foremost, Zango's notice and consent process would readily meet the requirements of H.R. 964 (as would its uninstallation and ad-labeling functions further described below). Specifically, prior to download and installation, the software displays to every potential user a conspicuous and plain-language description of the software and requires not one but two opt-in consents. It does this through a complex set of technologies that Zango invented for this very purpose, in response to concerns its executives heard beginning in 2004 from Members of this Committee, the Senate Commerce Committee, their respective staffs, and consumer advocates such as the Center for Democracy and Technology. Named Safe and Secure Search (S3), Zango's proprietary technology is designed to thwart the efforts of rogue individuals or entities that use botnets, Windows security holes, and other illicit means to attempt to fraudulently install software onto computers without user notice and consent. This technology has been a part of Zango's software installation requirements since September 2005. As of October 2005, Zango also ceased paying publishers for distribution of pre-S3 versions of its software. A new and enhanced version of S3, included as part of every download since January 1, 2006, features a closed-loop system that enables quicker detection of unauthorized attempts to install the software.

Second, Zango does not track or store *any* personally identifiable information (PII). Since H.R. 964 and its predecessors have been commonly referred to as "spyware" bills, it is important to emphasize that Zango does not collect a user's name, address, e-mail address, phone number, social security number, credit card number, or any other personally identifying information. In short, Zango is not spying on anyone. Zango's software uses only the non-PII data necessary to provide consumers with access to comparative shopping opportunities during their online search process.

This consists mainly of the momentary linkage of two data points – the URL address of the site the user visits, and the IP address of the computer being used. Even those two minor data points are not retained or stored.

Third, instead of merely providing hyperlinks in response to a search query, or simply serving the user with "click-throughs" or banner ads, Zango delivers an advertiser's Web site (or specific Web site page) in response and related to the consumer's search for a product or service, so that the user may directly access the advertiser's product. This business model avoids interrupting the user's enjoyment of non-transactional computer activity (during which time advertisements are not designed to be delivered) – for example, playing games, typing a document, or listening to music – and instead displays the advertiser's Web site or page only during Web browsing activity that would appear to have the highest relevance to the advertiser and consumer alike. This unique ad-delivery method, called "time-shifted advertising," separates the advertising experience from the content it supports and moves it to a time and context more valuable to the consumer receiving the message – providing the consumer with the benefits of comparative offers on the Web at a time the consumer is more likely to be shopping online.

Fourth, advertisement presentation on Zango is standardized so that consumers see competing Web offers in a separate browser window that are prominently branded with Zango's company name, the Web location from which its software was downloaded, and a link to its customer support page (which includes instructions for uninstallation of the software). To ensure that consumers are provided a safe, meaningful, pleasant and positive download and advertising experience, Zango requires its partners to follow both a Web Publisher Code of Conduct and an Advertiser Code of Conduct. Failure to abide by these Codes is cause for immediate termination,

forfeiture of any financial gains from illicit installations, de-activation of ad campaigns, and penalties.

Finally, Zango does not hide, as some advertising programs do, in a registry or file that makes it difficult for consumers to locate on their computers; instead, it provides a branded icon in the computer's "system tray" visible at the foot of the screen. It is also identified clearly on the list of programs the user can see when he or she clicks on the "Add or Remove Programs" menu. Consequently, the software can be easily uninstalled by clicking the "Remove" button next to the entry for Zango. In addition, the Frequently Asked Questions (FAQ) page on Zango's Web site also provides clear instructions and a link to "uninstall Zango." If issues or questions remain, the company also provides online customer support for its users 24 hours a day, seven days a week.

Zango Supports Most Provisions of H.R. 964

We commend the Subcommittee, and the full Energy and Commerce Committee, for its efforts to enact federal legislation that (1) protects Internet users from the ill effects of spyware programs; (2) requires clear and conspicuous notice, consumer consent, simple uninstallation procedures, and an ad-labeling function for programs that display advertising to consumers on their computers; and (3) provides a single coherent and pro-competitive federal regime for consumer protection in this area, rather than a patchwork quilt of differing state laws, some of which are motivated less by an intention to protect consumers than by a desire to protect favored home-state businesses from Internet competition.

The policy debate in this area has addressed not only privacy concerns about how computers may be secretly accessed and used by nefarious third parties, but also the belief in

some quarters that consumers simply dislike online advertising. Zango's experience challenges that belief, and it would point to the 20 million consumers who have knowingly and willingly installed Zango on their computers as strong evidence to the contrary. Moreover, online advertising is no less a legitimate form of expression protected by the First Amendment than advertising in the more traditional media, not to mention an essential means of providing useful information to the growing number of consumers who prefer to do their shopping online and sponsorship for the massive quantities of content that can be accessed online.

Nonetheless, Zango recognizes that concern over how some advertising has ended up on consumers' computers without their knowledge or consent is why H.R. 964, like most of its predecessor and companion bills, addresses downloadable programs that deliver advertising to consumers, and not just "spyware" – a pejorative term that should be limited to software that, *without notice and consent*, collects PII about the user, transmits PII to any third party, or engages in any deceptive, fraudulent, or dangerous action. And although as I emphasized above, Zango is *not* spyware, the company long ago recognized that its success, and ultimately the success of its business model, was dependent upon Internet users and consumers being able to understand and trust its value proposition, and upon a level regulatory playing field for all online advertising businesses. Thus, Zango has supported congressional action in this area and, as far back as the 108th Congress, specifically endorsed H.R. 2929 as reported by this Committee, a well-crafted measure to achieve the three goals described above.

Zango is pleased that the essential elements of that bill were incorporated into H.R. 29 during the 109th Congress and into the current Congress's H.R. 964, which we are discussing

here today. Zango strongly supports federal legislation to prohibit devious and fraudulent behavior with respect to the collection of PII or the secretive installation of software on users' computers.

H.R. 964's greatest strength is its recognition that the conduct and intentions underlying different forms of downloadable software require different legislative approaches. For example, not all software that serves advertising collects PII; Zango is an example of that. By contrast, there are many programs that collect PII and even sell it to third parties without ever serving a single advertisement. Many Web sites do both without ever giving the user notice or obtaining the user's consent.

Section 2 of the bill would absolutely prohibit the dangerous and pernicious practices that are most frequently associated with spyware – practices that, in fact, have contributed to unfounded and unfair suspicions about many other downloadable software applications including Zango's. Section 3 of the bill preserves consumer choice and consumer benefits for other downloadable software, including desktop advertising, by appropriately and carefully requiring clear notice, opt-in consent, easy uninstallation, and plain identification to the consumer of the source of an advertisement the consumer may be viewing. Zango supports these provisions, as well as the provisions of section 3 giving the Federal Trade Commission (FTC) authority to craft regulations to implement those requirements.

We also commend the authors of the bill for continuing to include the preemption provisions of section 6. While some states have moved to enact so-called anti-spyware laws, it is

widely believed that several of these were motivated more by a desire to protect powerful home-state business interests from online competition – to the obvious detriment of consumers – than to protect computer users from dangerous software. Even where no such intention exists, this Committee has wisely and repeatedly recognized that state-by-state legislation affecting online commerce is unwieldy, impractical, and ultimately confusing to businesses and consumers alike. The preemption provision of the bill appropriately continues in section 6(a)(3) to protect state trespass, contract, tort, and fraud laws. Still, Zango suggests that report language clarify the Committee's intention that states not be permitted to override H.R. 964's federal approach with contrary or additional requirements disguised to fit within one of section 6(a)(3)'s exceptions.

The authors of this legislation originally intended to address only the issues raised by downloadable software. Nonetheless, because Zango competes directly with other online business models that use Web sites rather than downloaded software to serve ads, it is useful to reiterate a point Zango has made in comments to the Committee on earlier versions of this legislation. The primary distinction between the manner in which these other business models generate their advertising revenues and Zango's business model is that Zango's conspicuously displays a notice to the consumer of what the consumer is getting and requires the consumer's explicit consent before that advertising is displayed. In stark contrast to that approach, which collects absolutely no PII, many popular Web sites require a user to provide a variety of personal information in order to visit those sites. These Web sites then use that personal information to serve advertising to the users, and even transfer that information to third parties for use in other advertisers' programs, whether the user has consented to it or not. Zango acknowledges that this bill will not directly address the privacy concerns inherent in those marketing practices but, in

the name of competitive parity, Zango commends the Committee for seeking from the FTC, in section 8, a report on the use of tracking cookies in the delivery and display of online advertising.

The Liability Exception in Subsection 5(c) Should Be Stricken

Zango is concerned by subsection 5(c) of the bill, which has been described as a liability exception for so-called "good Samaritans." Although it was undoubtedly well-intended when it first appeared in the 109th Congress's H.R. 29, it is potentially both anticompetitive and, based on Zango's own experience, subject to commercial abuse. Some companies selling scanning applications to consumers compete with each other by issuing inflammatory warnings designed to frighten consumers about software "lurking" on their computers. Rather than assisting Internet users and consumers, the liability exception provided by subsection 5(c) – and by most other versions of a so-called "good Samaritan" provision that were discussed in the last Congress – could primarily end up serving the interests of the most aggressively marketed scanning applications. If not deleted, H.R. 964's liability exception may also distort the market for online advertising dollars in an anticompetitive manner, mainly to the benefit of large companies that compete with the much-smaller Zango. Zango urges the Committee to strike it from the bill.

At a minimum, even if read most narrowly to be limited strictly to actions taken by the FTC, the provision unnecessarily restricts the FTC's ability to pursue enforcement against those parties the FTC believes warrant it. Equally important, the presence of such an immunity provision in the bill opens the door wide to judicial application and expansion of the concept in private litigation between commercial parties. It will not be long before a purported

"congressional policy of protecting good Samaritans" is cited by a scanning application in a court of law as the basis for dismissing or defending against a civil claim that the scanning application has misidentified, mislabeled, or even commercially defamed a useful item of software, including perhaps even another scanning application.

This is more than just a hypothetical concern for Zango. Regrettably, the company has had direct experience, including litigation, with the kind of software provider that would argue for legal immunity under a logical extension of a provision like this. As difficult as the experience was for all concerned, the relevant point here is that Zango's filing of a lawsuit ultimately had the desired effect – forcing the scanning application to alter its mischaracterizations and enabling Zango to remove the sole impediment to an important business deal. If subsection 5(c) had been federal law when Zango's interaction with this scanning application provider began, the provider might have felt far more comfortable adhering to its position. At a minimum, it could have constructed a plausible legal and policy argument for an affirmative defense of immunity that could have prolonged the litigation until a fact-finder had the opportunity to decide whether it had acted "in good faith" – a highly subjective standard that, as any litigator knows, can be difficult to disprove.

Multiply this single incident by dozens of software providers battling dozens of scanning applications in court, and subsection 5(c) could have the unintended consequence of promoting many more protracted legal battles over how the scanning applications label or characterize software. If this provision became law, it is reasonable to foresee state courts having to consider and decide whether the particular sensitivity that Congress evinced in H.R. 964 for these so-

called "good Samaritans" suggests a policy that would support extending such immunity to those scanning applications as a common law defense under state law. Legitimate software providers could well see their businesses harmed in the process, as Zango did, while the legislation unintentionally facilitates the typical scanning application's business strategy of attempting to gain market share by claiming to find more, and more allegedly damaging, software on the customer's computer.

In summary, when it comes to scanning applications, experience tells us the following:

1. Scanning applications get it wrong . . . a lot.
2. Scanning criteria are far more subjective than most scanning application companies would have you believe.
3. Fear mongering is a standard "tool of the trade" in the scanning application market.
4. Recourse against scanning application vendors is difficult and expensive – and could become more so if subsection 5(c) were enacted into law.

Scanning applications are not the only businesses that have a financial interest in interfering with advertisers' ability to work with companies like Zango to reach consumers. Many large and small online service providers, Web sites, and contractors serving those parties profit from their own competing online advertising models. Companies actively pushing the use of their own free ad-supported software and Web sites have every incentive to engage in and to continue the same sort of fear-mongering that benefits the scanning applications. And the same legal arguments could be made by those companies in litigation as the grounds for an affirmative defense of "good Samaritan" immunity. Based on Zango's own experience – including experience dealing with some companies that possess enormous economic power in the online marketplace – it can readily foresee some of those companies using this provision in an effort to

cripple desktop advertising software and thus eliminate a form of competition for advertising dollars that is arguably much more transparent to the consumer than the models they use.

Immunity grants in federal legislation are generally confusing at best, and ill-advised in most instances. There is no compelling reason in this case to alter the usual understanding that commercial disputes between commercial parties should be settled commercially, and that the conduct of commercial parties subject to the jurisdiction of the FTC is not entitled to a blanket exception from FTC enforcement merely because of the particular product or service being sold.

The passage of time since the House's consideration of H.R. 29 in 2005 has provided an excellent opportunity for further analysis of the "good Samaritan" concept and of the legislative language repeated in H.R. 964. Zango respectfully hopes that the preceding discussion will persuade the Energy and Commerce Committee to delete subsection 5(c) in any Managers' Amendment that may be offered during Subcommittee or Full Committee markup. With that single revision, Zango would strongly support passage of the legislation as introduced

Zango's FTC Settlement

Last week, following a public comment period and by a unanimous vote of 5-0, the FTC issued a final approval of the settlement it initially reached with Zango last fall. The settlement followed an investigation in which Zango cooperated fully. The investigation focused primarily on the company's alleged business practices during a period very early in its history during which it relied on outside affiliates to enforce its consumer notice and consent policies. Unfortunately, the company's management began to learn even before the FTC commenced its

inquiry that its early business model allowed deceptive third parties to exploit the company's system to the detriment of consumers, advertisers, and publishers. For Zango, which was founded by two childhood friends and, like so many Internet start-ups, grew more quickly than they had ever imagined possible, it was a painful lesson in who to trust. When the preliminary FTC settlement was announced last October, CEO Keith Smith publicly apologized for the resulting negative impact on those consumers, advertisers, and publishers who were adversely affected by any unwanted downloads.

Although the settlement requires Zango to adhere to a set of standards outlined in the order that are fully consistent with the requirements of H.R. 964 and to pay a $3 million penalty, two additional points are essential to note.

First, the agreement was made for settlement purposes only and does not constitute an admission that the law, as it stood at the time of the allegations, was violated. In essence, the FTC staff's complaint charged Zango with responsibility for its failure to anticipate the unscrupulous actions of some deceptive third parties. The company felt it best under those circumstances to apologize to anyone who had been harmed, pay the fine, and welcome the FTC's consent order – which included provisions that were in accord with Zango's current business model – as a template for the industry standards and best practices.

Second, more than a year before the FTC even began its investigation of past practices, Zango's management recognized that the online business of downloading software and applications needed a set of rules or guidelines with which all should comply. As a result of

their discussions with policymakers and public interest advocates here in Washington as far back as 2004, they began working with a number of inter-industry groups to develop best practices that required informed notice and consent for consumers. As noted earlier, they advocated for federal legislation to govern downloadable software practices. And on January 1, 2006, more than 10 months before the proposed FTC settlement was announced, they retired the distribution of their past products.

As of that date, they required that all Zango applications include an enhanced version of their proprietary Safe and Secure Search, or S3, technology. That new version included a built-in software enhancement, known as their Closed Loop System, that enables quicker detection of unauthorized attempts to install their desktop advertising software. They overhauled their distribution channel to completely eliminate third-party software distribution. They assembled an aggressive team of security professionals dedicated to the monitoring of the Zango software system 24 hours a day, 7 days a week, 365 days a year.

As a result of these efforts, Zango met or exceeded the key notice and consent standards detailed in the FTC settlement order literally months before that order was proposed, and the company now meets every other FTC requirement as well. While it may seem counterintuitive for Zango to welcome an FTC settlement under which it agreed to pay a $3 million fine, that is indeed the case because Zango views the FTC's standards as a set of best practices and a significant step forward in terms of providing legal clarity for the online advertising industry and, indeed, for all who offer downloads over the Internet.

Conclusion

The time has come for all online marketers to embrace and implement these standards as Zango has, but unfortunately not all will. Too many, in fact, will not until they are compelled to do so by new laws, regulations, or FTC orders that apply not only to Zango but to them as well. As the desktop advertising industry continues to evolve, Zango will continue to strengthen its business practices and enhance its technology to make the online economy increasingly valuable for everyone by enabling consumers, advertisers, and publishers to reach each other. With the single modification Zango has suggested above, H.R. 964 offers the promise of extending needed consumer protections across the online economy so that online commerce and content may continue to thrive and prosper in an atmosphere of trust.

Thank you again for inviting Zango to participate in today's hearing and for your consideration of its views.

Mr. RUSH. Thank you very much.

The chair recognizes himself for 5 minutes of questioning. I am going to ask a series of questions of this entire panel and I ask you in the interest of time, I only have 5 minutes, that you do not filibuster, just answer the question with a yes or no answer. I will give you ample opportunity if I have time remaining to expand on your answers after we have gone through this entire series.

So I want to start with Mr. Schwartz. Mr. Schwartz, do you support H.R. 964?

Mr. CERASALE. Not as written.

Mr. RUSH. Mr. Morgan?

Mr. MORGAN. On behalf of TACODA, we support the bill.

Mr. RUSH. Ms. Maier?

Ms. MAIER. Yes.

Mr. RUSH. Ms. Varney?

Ms. VARNEY. Yes.

Mr. RUSH. Next question. Do you believe that consumers should be protected from the dangers of significant economic losses inherent in spyware programs, and if your answer is yes, do you support section 2 of the bill?

Mr. Schwartz?

Mr. SCHWARTZ. Yes, and yes.

Mr. RUSH. Mr. Cerasale?

Mr. CERASALE. Yes to both.

Mr. RUSH. Mr. Morgan?

Mr. MORGAN. Yes to both.

Ms. MAIER. Absolutely.

Ms. VARNEY. Yes to both.

Mr. RUSH. Do you believe that consumers should receive clear and conspicuous notice of advertising and tracking software, especially programs that collect personal information on consumers, Mr. Schwartz?

Mr. SCHWARTZ. Yes.

Mr. CERASALE. Yes, Mr. Chairman.

Mr. MORGAN. Yes, Mr. Chairman.

Ms. MAIER. Yes.

Ms. VARNEY. Yes.

Mr. RUSH. I am tempted to start from this end but I am winning starting from that end so I think I am going to keep on going. I am not going to change.

Do you believe that consumers should be provided the right to consent to such intrusive applications on their computers?

Mr. SCHWARTZ. Yes.

Mr. CERASALE. No, we believe in consumer choice, not necessarily one size fits all.

Mr. MORGAN. On behalf of the IAB, we believe that one size does not fit all.

Mr. RUSH. So what is your answer?

Mr. MORGAN. My answer would be no, not broadly.

Ms. MAIER. Yes.

Ms. VARNEY. Yes.

Mr. RUSH. I am going to start at this end now.

Ms. Varney, do you believe that such programs should provide consumers with a simple installation procedure?

Ms. VARNEY. And simple uninstallation, yes.

Ms. MAIER. Agree with that, yes.

Mr. MORGAN. Yes.

Mr. CERASALE. Yes, it should be if they can't fully uninstall, it should be at least totally disabled.

Mr. SCHWARTZ. Yes.

Mr. RUSH. Ms. Varney, do you support section 3 of the bill?

Ms. VARNEY. Yes.

Ms. MAIER. Yes.

Mr. MORGAN. And as I said before, yes, TACODA is supportive of the entire bill. On behalf of the online advertising industry, we would like a few parts of section 3 re-examined.

Mr. RUSH. Mr. Cerasale?

Mr. CERASALE. Section 3, not totally as written.

Mr. SCHWARTZ. We support the goals of section 3. We have some comments in our written testimony regarding some of the details.

Mr. RUSH. Ms. Varney, do you believe that the Congress should provide a single, coherent, pro-competitive regime for consumer protection in this area rather than a patchwork quilt of different State laws?

Ms. VARNEY. Yes, I do, Chairman.

Ms. MAIER. Yes, I do.

Mr. MORGAN. Yes, I do.

Mr. CERASALE. Yes, we support preemption.

Mr. SCHWARTZ. In general, yes.

Mr. RUSH. Mr. Schwartz, I have a few moments.

Mr. SCHWARTZ. I would say that we would like the States to be able to act under the Federal bill though. I understand that that raises some jurisdictional questions but we hope that that can be addressed on the floor that attorneys general will be able to act under this bill as a Federal bill.

Mr. RUSH. We have had some earlier commentary on the Good Samaritan provision. Is there anybody else that would like to add some other commentary on the Good Samaritan provision?

Mr. SCHWARTZ. I will make a statement about the Good Samaritan provision. I think that the goals of the Good Samaritan provision are good ones. The goals seem to be to promote anti-spyware software. Really, the first line of defense for a consumer today is anti-spyware software and we have seen that it has had a major effect, positive effect on the issue. I have worked with the anti-spyware coalition, with anti-spyware groups and with privacy groups and public interest groups, working together to build best practices and standards for how anti-spyware companies work. We think that we have come up with a good set of best practices, putting out more actually just today that have gone through an extensive public comment period.

I question the concern over the provision, more because I don't think it is going to be effective in doing what the goals intend it to do. The goal is, as I said, to promote anti-spyware software but it really only protects anti-spyware software from the provisions, from the penalties in the bill and not from things that an anti-spyware company is most likely to be sued over, defamation, for example, or raising concerns about software. There are no penalties in this bill that go after anti-spyware software in that way so I

question how effective it is going to be, but the concerns that have been raised here I don't see as really getting at the main problem with the provision.

Mr. RUSH. My time has expired.

Now I will recognize the ranking member, Mr. Stearns.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. Schwartz, you mentioned in your opening statement that sometimes it is so difficult to get rid of the spyware that you have to throw away your computer and there is not really a program out there that can just sweep through and get rid of the spyware?

Mr. SCHWARTZ. We have seen a real increase in the ability of these programs to embed themselves in computers.

Mr. STEARNS. So it is almost impossible to get rid of them?

Mr. SCHWARTZ. In many cases, if they have something that is called a root kit, it can be imbedded into the operating system, so when you are looking for the program, you ask the operating system, the operating system basically tells you this program isn't there because the question goes to the operating system and the root kit basically tells the operating system—and this is a very simplistic version of what happens but——

Mr. STEARNS. With that in mind, I ask the staff, there are only four States in the United States that have actually passed spyware: New York, Texas, California and Washington. Utah tried to do it and the courts threw it out. What was the reason why the courts threw it out? Does anyone in the panel know?

Mr. SCHWARTZ. It was a different kind of a spyware bill. It really tried to focus on copyright provisions, intellectual property of ads showing up over the other ads, the place where the consumer was trying to go instead of at the deceptive practices that this bill and that most of the other bills have gone after.

Mr. STEARNS. Ms. Maier, some critics have suggested that the online environment has changed with new software, new programming so that this legislation really perhaps is not needed, and maybe, Mr. Schwartz, you can help me too. Do you think that it is possible that it would be accurate that—there are some software companies that are not in favor of this bill. Some of them are concerned because we have a study on cookies and others are concerned, say well, just let the software handle it. What is your opinion in terms of software being able to prevent software from coming in and that would take of the problem, we don't need legislation?

Ms. MAIER. Sir, there is always the good players and the bad players and I think the good players can look to self-regulatory efforts, to look to best practices and——

Mr. STEARNS. So there is no software out there that would prevent the bad players from getting into the computer?

Ms. MAIER. I don't think there is a perfect solution. I think it really is a partnership between legislation, technology, self-regulatory and other efforts, and so I see legislation as necessary.

Mr. STEARNS. Does the rest of the panel agree with that, that there is no software out there that at least would cover 90 percent of the spyware?

Mr. SCHWARTZ. That is correct.

Mr. CERASALE. That is correct. As a matter of fact, if there were one tomorrow, it might not be effective as technology is constantly changing.

Mr. STEARNS. So as much as technology is moving forward for software, bad guys can find another way?

Mr. CERASALE. Absolutely. They may be more technologically advanced the more people are trying to stop them.

Mr. MORGAN. Yes, I would agree with that. I mean, it is absolutely impossible for technology to be a silver bullet here.

Mr. STEARNS. Ms. Varney?

Ms. VARNEY. I agree with that.

Mr. STEARNS. OK. The next question is, it appears that section 3 of this bill is the area that a lot of people are concerned about. I guess for the panel, are cookies used for the purpose of serving advertisements? Should cookies be treated differently than spyware that does not use personally identifiable information to serve advertisements?

Mr. Schwartz, would you start?

Mr. SCHWARTZ. Cookies are a somewhat complex issue but I do think that they should be treated differently than software.

Mr. CERASALE. Cookies are so much embedded in how the Internet works. It clearly is a different animal. Cookies and similar-type technologies are different from a software download.

Mr. STEARNS. OK. Mr. Morgan?

Mr. MORGAN. Yes, cookies and what I would call relatively passive technologies are very different than the kind of invasive software that has been used with the computer programs. I think the issues that people have around section 3 are, it is really hard to figure out the wording of how you can get between that passive and active from a practical standpoint.

Mr. STEARNS. Mr. Morgan, when this got out of our committee, they put in this study on cookies, and I cautioned them, I said that was going to create a lot of concern and angst in the industry because once you have a study on cookies, the study might come out, you never know where it is going to go and everybody has these cookies. Do you think cookies by themselves are innocuous and——

Mr. MORGAN. I think they are largely innocuous but I actually think that the study is a fine idea. I think that this is one of those examples, as they say, that sunshine is the best antiseptic. If there are problems, I don't think anything is hurt by having attention brought.

Mr. STEARNS. Ms. Maier, and you might also point out, answer the first question, but the second intuitively is this study on cookies, is that necessary?

Ms. MAIER. First of all, I think that cookies are outside the scope of what we call software or downloadable applications in our program. A study on cookies I think is a great idea. I think there are a lot of things going on. Our Web cell program requires consumers to know about other cookies and other tracking software so if there is a study on cookies, I hope it would be including other——

Mr. STEARNS. Is it possible cookies could replicate the software once they are in the computer?

Ms. MAIER. What it is technically possible continues to amaze me but I don't think that is——

Mr. STEARNS. Do cookies track and do the same thing that spyware does in another way that could be considered harmful?

Ms. MAIER. Not generally.

Mr. STEARNS. Mr. Schwartz, do you want to answer that?

Mr. SCHWARTZ. Cookies basically give an ID number from a particular Web site and they can be used—the uses of them have changed over time and—but there are more harmful pieces of ID tracking that have come up over time so it is kind of—there has been a change in that. I do think that a study would be helpful at getting at how they are being used.

Mr. STEARNS. Ms. Varney, let me just close. My time is running out. If you don't mind just answering the question.

Ms. VARNEY. Sure. I think the study is a terrific idea. I think the tension around section 3 is on two levels. Cookies, java script, HTML, all devices used in the seamless delivery of content that consumers want today on the Internet can be abused, and the question is, where does this bill land on those type of seamless technologies.

I think there is another tension maybe unspoken in public. Yahoo, Google, AOL all have toolbars and those toolbars absolutely collect information and deliver advertising. Currently, those companies give you great notice and get great consent inside their master agreement. They don't pull it out separately. I think there is a question about whether or not they should and whether or not that bill requires them too.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. RUSH. Ms. Schakowsky is recognized for 5 minutes.

Ms. SCHAKOWSKY. Mr. Schwartz, you frequently talk about baseline privacy legislation and I wondered if you could describe for us what you would envision for such a bill and also because you mentioned—I can't remember if you said it but in your written testimony there are some downsides to not having a more comprehensive piece of legislation in dealing, for example, with spyware alone. So I wonder if——

Mr. SCHWARTZ. Let me start with the problems and then move to what we would like to see. Some of the problems that we see, you have different—we start coming up with these different privacy bills in all of these areas, I mentioned seven in my testimony, but for those of you who have been on this subcommittee know, there are dozens, literally dozens of privacy issues that have come before this subcommittee over the past 10 years or so, as we start coming up with different standards for different types of information, it becomes harder for consumers to know what the particular standard is for that type of information. If we don't have a safety net there, and there are some areas that still fall outside of that so a new technology arises and you have to create a new standard for that new technology. You have to compare it to all these other differing standards, go through this whole process again. We think that it makes more sense to come up with really a baseline safety net kind of standard where we know that if something falls out of it, at least it is covered by this new standard of where personal information is being directly collected, and we would like to see something that covers the fair information practices. I think that the Federal Trade Commission, actually started by the work of Commissioner

Varney at the end of the table over there, has at one point back in the 1990's endorsed privacy legislation. We thought that that was an excellent starting point: notice, choice and consent, depending on the situation, access and security and enforcement as a great starting point to look at to getting at these issues. We feel there have been a number of bills over the years that have started us down that path. We now have 13 companies that testified in front of the, I think it was the full committee, last year in support of looking at general privacy legislation. We think consumer groups are behind it. There is momentum now we think to get at this issue so that we don't have these kind of different standards across different kinds of industry, across different kinds of technology.

Ms. SCHAKOWSKY. I would really like to hear from other panelists on their view of having a comprehensive baseline bill.

Mr. Cerasale?

Mr. CERASALE. Yes. Well, DMA does not have a set position on an overall comprehensive privacy bill. We want to be open and talk and discuss it. There are an awful lot of privacy laws in the United States and how they do come together and so forth and what information is covered and not covered. An overall privacy bill could in fact really create the different standards that financial information is treated one way whereas as marketing information another that may be more restrictive and so it is a very complicated issue and we have an awful lot of guidelines. It is not just DMA but OPA and others have guidelines that companies like Yahoo, AOL and Google follow with notice and choice and I think that right at the moment you have in the United States a series of laws and guidelines as industry works together that seems to work. One of the problems with an overall bill is that technology is changing so quickly, it makes it very difficult as we see, for example, the computer——

Ms. SCHAKOWSKY. I am going to have to stop you because I want others to speak. But it is also a problem with technology changing with very specific bills that deal with a specific problem.

Yes?

Mr. MORGAN. Both TACODA and IAB, we don't have a formal position but we are certainly open to dialog on that kind of legislation.

Ms. SCHAKOWSKY. Ms. Maier.

Ms. MAIER. We have been working with a number of companies in trying to encourage better privacy protections for consumers and in general we think baseline privacy legislation could be good. That said, I think we still need spyware legislation because a lot of this doesn't even have to do with personal information but computers installing things and tracking and that could be outside the scope of privacy legislation.

Ms. VARNEY. Congresswoman, I am here on behalf of Zango and they really have not examined whether or not it would be for or against any baseline privacy legislation. They strongly support this bill and they don't collect personally identifiable information. So I think there is a need—even if there a baseline privacy bill that we get out of the Congress and signed by this President, there probably still is a need for this type of legislation.

Ms. SCHAKOWSKY. I am not suggesting that we don't do this legislation. Thank you.

Mr. RUSH. Mrs. Bono is recognized for 5 minutes.

Mrs. BONO. Thank you, Mr. Chairman.

First, I just want to comment on the discussion about cookies. I think the study or the report on cookies in the bill is a good thing and I didn't really have a problem with cookies in the beginning because anybody with a slightly elevated degree of sophistication on the Internet knows how to go ahead and delete your cookies. It is not that hard to do. So I think the report obviously is a good thing. That is why we didn't really give it more weight than that because there is a removal tool.

And I just want to comment, the question that Ranking Member Stearns asked was about software and how effective it is at removing spyware/adware and I just want to applaud Microsoft because I think Windows Vista—I am a user of Vista on one of my computers—and I think they have come a long way and with Windows Defender I think they have certainly tried to tackle the issue. As soon as Windows Vista works with iTunes, it might be a perfect world, but until then, I do want to applaud them for their efforts to address the issue.

But I would like to ask a question of Mr. Morgan, and that is, can you tell us about the current state of the online advertising industry and how popup ads are currently being used? There has been obviously a lot of restraint, best practice put into place but they are still out there. Can you go over what they are doing now?

Mr. MORGAN. Certainly, Congresswoman. Well, first I would like to say I have been in the online advertising industry for about 15 years and we have probably had some forms of spyware for the better part of the last 10, and I applaud you, Congresswoman Bono, because until you made it an issue and brought it to the forefront, it wasn't being talked about, and I won't say it wasn't being talked about in Congress. It wasn't being talked about inside the online advertising industry. I am one of the first to say self-regulation and self-regulatory practices help solve problems but we weren't solving it, and that is one of the reasons you probably hear sometimes a little balance of my position in TACODA in talking about other things. But I will say that since you got involved and you and Congressman Towns introduced the bill, there has been a lot of attention in the industry and I have not seen any issue that has had more attention in the industry over the last several years, and what we have seen is, we have seen a significant, I would say a dramatic reduction in the use of popup advertising. We have certainly seen companies like Microsoft make extraordinary leaps forward in software and technology. We have seen a lot of practices go forward and I think that has been a great thing.

Mrs. BONO. Can you describe then how interactive advertising helps provide consumers with free online content?

Mr. MORGAN. I think that—and this is a tiny anecdote but one of the things I have found in talking to people about this is that a lot of people think the Internet works like cable television and that you pay a bill to an Internet service provider and you get access to a bunch of channels and content, and what most people haven't realized is the money that is paid by a consumer never actually makes it to the people that make the content. Not a penny of that goes to the New York Times or to Orbitz or to iVillage. They

are 100 percent supporting what they give for free to consumers with advertising and one of the reasons it has been such a robust industry that we have really supported the actions against spyware because it had the capability and still has some capability that really had the capability to really harm or destroy what was really emerging in strong industry.

Mrs. BONO. I think on your point there, I just picked up—the committee did a great job providing a ton of information up here including a Business Week article from July 17. I hadn't even seen this before, but for those of you who have seen it, the opening quote says consumers have strong opinions about direct revenue software, and this is a quote: "If I ever"—I don't even know if I should say this for the record but it says, "If I ever meet anyone from your company, I will kill you," a person who identified himself as *X* said in an e-mail to Direct Revenue last summer, "I will ****kill you and your families." That is what it says. Such sentiments aren't unusual. "You people are evil personified," and this gentleman goes on to say, "I would like the 4 hours of my life back I have wasted trying to get your stupid uninvited software off of my now-crippled system," and I think that last sentence really identifies people's frustration with adware and spyware and it is not a matter of direct advertising and good practices. It is a matter of really interfering with people's lives and the fact is I believe we own our own computers, not an outside source, and that is where this whole thing came from.

I see Mr. Chairman, that I am just about out of time and I just want to thank all of you on the panel who have worked with us in the past on this bill and I know Ed Towns and I will continue to work with you and hear your concerns as we go through the process. So thank you very much.

Mr. RUSH. Does the gentlelady request unanimous consent that this be included into the record, the article?

Mrs. BONO. Yes, Mr. Chairman, thank you, and also to notice that I was quoting because I don't know if I violated rules by quoting the F-word but I did not say that word so I don't want to get in trouble.

Mr. RUSH. No, since you complimented the committee, we will accept that. Thank you.

Mr. RUSH. Ms. Hooley, you are recognized for 5 minutes.

Ms. HOOLEY. Thank you, Mr. Chairman, and I thank all of my colleagues who have worked so hard on this bill and Mrs. Bono, for all of your hard work.

I am a cosponsor of the bill. I strongly support this bill and I want to make sure there are not any unintended consequences and I am concerned that there may be unintended consequences if there is detection software, then that they can't be used to keep consumers safe them from fraudulent activity. I know, Mr. Chairman, you pointed out the exemption clause but I don't know if that clause actually does what it needs to do to make sure that there is an exemption here for the software that helps keep fraudulent activity out of your life, software that determines the legitimacy of a transaction or to verify information supplied by that consumer, and I guess I would like to hear from you if you think again that we don't have some unintended consequence in this piece of legislation.

Ms. VARNEY. May I comment on that?

Ms. HOOLEY. Yes, please.

Ms. VARNEY. Zango has commented on that provision, Congresswoman, and the way that we read the language, and if I may, I will just quote it. It says that "No provider of computer software may be held liable under this Act on account of any action voluntarily taken or service provided in good faith to disable a program used to violate section 2 or 3." There is a couple of concerns we have. Remember, this Act is enforceable by the FTC.

Ms. HOOLEY. Right.

Ms. VARNEY. It doesn't create a private right of action. So what this in effect is saying to the FTC is that anybody can hide behind the defense of hey, we are just a scanning ap trying to take bad stuff off people's computers. We think that is an unwise standard to put in this Act. The FTC is very judicious about its enforcement and I cannot foresee a circumstance under which they would go after a legitimate provider of a scanning application. However, the providers of scanning applications ought to be under the same requirements when it comes to notice and consent and uninstall. So we think that the better course here, since this is an act empowering the FTC to prosecute bad actors, is to leave that exemption out, let the FTC prosecute those who do have the requisite bad intention or who fail to provide the adequate notice, consent and uninstall.

Ms. HOOLEY. Yes, Mr. Cerasale?

Mr. CERASALE. I want to look at the exemption provision in section 5(b) where the monitoring or interaction of your anti-fraud software you are exempted from the Act totally so in the notice and all of that but it is limited to telecommunications carrier, cable operator, computer hardware or software provider or provider of information, service or interactive computer service to the extent that it is more for anti-fraud. Those are not the only people—they are not really software providers. They are not the only people running the anti-fraud programs, creating the software and sending it in. So we need to expand to financial institutions to use this, credit card companies, so forth, retailers even use because they collect credit cards or direct marketers so we need to look at expanding 5(b), not that the exemption is bad but to expand it to help us in the prevention of financial fraud.

Ms. HOOLEY. OK. I am assuming that you would have a list of what else needs to be added to those exemptions?

Mr. CERASALE. Yes. I will provide that list and try and work out—we probably need to talk with committee staff to make sure that we are as inclusive or not too inclusive in the exemption.

Ms. HOOLEY. Did this fix this in the Senate, by the way? Did they do something different in the Senate, anybody know?

Mr. CERASALE. They did make a change in the Senate so we can use—we will provide the Senate language.

Ms. HOOLEY. OK. Thank you.

Mr. RUSH. Thank you so very much. I certainly want to extend our thanks to the witnesses who have come and helped us and informed us so much and participated in this hearing. Again, thank you for taking the time out from your busy day.

With that said, we will call the committee adjourned. The committee is now adjourned.

[Whereupon, at 12:30 p.m., the subcommittee was adjourned.]

○