AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 106–815

PRIVACY IN THE DIGITAL AGE: DISCUSSION OF ISSUES SURROUNDING THE INTERNET

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

ON

PRIVACY ISSUES SURROUNDING THE INTERNET, FOCUSING ON INTERNET INDUSTRY POLICY, SECURITY, DATA PROTECTION, LAW ENFORCEMENT, TECHNOLOGY DEVELOPMENT, AND ELECTRONIC COMMERCE

APRIL 21, 1999

Serial No. J–106–19

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
68–199 CC WASHINGTON : 2001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JOHN ASHCROFT, Missouri
SPENCER ABRAHAM, Michigan
JEFF SESSIONS, Alabama
BOB SMITH, New Hampshire

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ROBERT G. TORRICELLI, New Jersey
CHARLES E. SCHUMER, New York

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Hatch, Hon. Orrin G., U.S. Senator from the State of Utah	1
Kohl, Hon. Herbert, U.S. Senator from the State of Wisconsin	3, 4
Leahy, Hon. Patrick J., U.S. Senator from the State of Vermont	16, 18

CHRONOLOGICAL LIST OF WITNESSES

Panel consisting of Katherine Borsecnik, senior vice president, Strategic Businesses, America Online, Inc., Dulles, VA; Michael Sheridan, vice president, Strategic Businesses, Novell, Inc., Orem, UT; Irving Wladawsky-Berger, general manager, Internet Division, IBM Corp., Washington, DC; Jerry Berman, executive director, Center For Democracy and Technology, Washington, DC; Russell T. Bodoff, senior vice president and chief operating officer, BBBOnline, Inc., Arlington, VA; and Gregory Fischbach, chairman and chief executive officer, Acclaim Entertainment, Glen Cove, NY 7

ALPHABETICAL LIST AND MATERIALS SUBMITTED

Berman, Jerry:	
Testimony	65
Prepared statement	67
Bodoff, Russell, T.:	
Testimony	71
Prepared statement	73
Appendix: BBB*Online* Privacy Programs, Compliance Assessment Questionnaires and Flow Charts	79
Borsecnik, Katherine:	
Testimony	7
Prepared statement	9
AOL's, Certified Merchants Program	13
Fischbach, Gregory:	
Testimony	171
Prepared statement	172
Sheridan, Michael:	
Testimony	20
Prepared statement	21
Wladawsky-Berger, Irving:	
Testimony	25
Prepared statement	26
Exhibits: IBM's Privacy Practices on the Web	34
OPA Whitepaper: Online Consumer Data Privacy in the United States	48

APPENDIX

ADDITIONAL SUBMISSIONS FOR THE RECORD

Letter to Senators Hatch, Feinstein and Leahy, accompanied by AOL's Terms of Service (which includes the AOL Member Agreement, the AOL Community Guidelines, and the AOL Privacy Policy), as well as a copy of AOL's guidelines for using "parental controls" to protect children online, submitted by Jill Lesser, vice president Domestic Public Policy, America Online, Inc., dated April 23, 1999 207

PRIVACY IN THE DIGITAL AGE: DISCUSSION OF ISSUES SURROUNDING THE INTERNET

WEDNESDAY, APRIL 21, 1999

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The committee met, pursuant to notice, at 10:03 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch (chairman of the committee) presiding.

Also present: Senators Thurmond, Leahy, Kohl, Feinstein, and Schumer.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

The CHAIRMAN. Good morning, and welcome to today's hearing addressing the important and increasingly complicated issue of privacy on the Internet.

It has been no secret that throughout my career in the U.S. Senate, I have advocated and sought policies that encourage and foster the development of new and better technologies. Included among them are medical technologies that help to improve the health of Americans and information technologies that bring distance learning to many who live in rural areas in Utah and across the Nation. The Internet's explosive growth promises to impact every aspect of our daily life, as it provides the public with useful and often vital information and literary content immediately at the mere click of a mouse.

Internet technology will play an important role in educating the population through distance learning and through the general delivery of information. The Internet will also continue to play an increasingly larger role in our daily entertainment, whether it is through the delivery of movies and music over the Internet or through the ability to play video games with a network of literally millions of players across the globe.

During the last session of Congress, I worked with my colleagues on this committee in a bipartisan manner to act on a number of matters aimed at fostering the growth of the Internet and promoting a competitive environment in this new digital environment.

First, this committee won passage of the Digital Millennium Copyright Act, which put in place the most significant revisions to the U.S. copyright law since the enactment of the 1976 Copyright Act. I consider that one of the most important bills of the whole last session.

Second, the Judiciary Committee initiated the still ongoing, thorough public examination of important issues affecting competition and innovation in the digital marketplace. In addition, the committee also provided legislative assistance to industry in our national effort to prepare for the Y2K problem by crafting and passing legislation to allow businesses and local governments to share Y2K remediation information with limited fear of liability.

During this session of Congress, I intend to continue working on legislative and oversight efforts that address new policy changes of the Internet and the new digital revolution. Today's hearing is the first this committee has held on the issue of consumer privacy on the Internet. Given the complex nature of this issue and all of the various policy considerations involved, I do not expect this to be our last hearing on this issue.

Any revolutionary, paradigm-shifting technology presents government with new and significant policy changes and challenges. The Internet is no exception. I recently read that earlier in this century there were concerns about the sale of automobiles to the public as it provided crooks with a tool to escape the police. Luckily, we found a way to address this automobile, "concern." It is my hope that we can do the same for any concerns that surround the Internet.

As Americans spend more of their lives on the Internet, they are more concerned about the ability of Web sites, both government and commercial, to track their, "digital steps." There is no question that in order for the Internet to reach its maximum potential as a viable avenue for transacting commerce, consumers must be assured that personally identifiable information that is collected online is afforded adequate levels of protection. But the question remains how do we best do that. How do we do it without chilling the development of new technologies or the expansion of the marketplace?

There have already been over 50 legislative proposals offered this session addressing privacy. I have been skeptical of most proposals to date, as they require increased regulation of the Internet by government. As I have expressed in the past, we must be careful not to stymie the growth of new technologies with broad government regulations.

The purpose of today's hearing is two-fold. First, it is intended to educate the public and the members of this committee about what the privacy issues are that surround consumer use of the Internet and what industry is doing to correct these problems.

Second, it will allow us to begin a dialogue with those with an interest in the privacy issue in order to develop a meaningful and balanced policy that takes into consideration the needs of consumers, law enforcement and industry, one that would ensure continued technology development in this important area and that ensures electronic commerce is able to reach its full potential.

Now, I believe that it is in the best interests of the industry to develop meaningful privacy policies and to provide adequate protections for consumer privacy. After all, individual consumers will demand that the electronic marketplace provide adequate and effective privacy protections.

Indeed, I have been very encouraged to see, in over the past 6 months, the development of a productive and meaningful effort by industry to ensure such privacy protection. We will hear testimony from some of those involved in that effort today. However, I am still concerned about reports that there might still remain certain fringe operators of Web sites who might not abide by the standards that the industry has set for itself. Any successful self-regulatory model needs to have adequate resources to enforce the rules that it sets for itself.

To date, the discussions surrounding Internet privacy have revolved around two mutually exclusive models as possible solutions to this issue. The first, advocated by certain consumer rights groups, would give government regulatory bodies the authority to regulate conduct on the Internet. And the second, advocated by most members of the industry, would entrust the industry to regulate itself without any role for the government. For the past several months, I have been examining different self-enforcement systems that have proven successful in other industries and that might serve as a useful model for the protection of privacy on the Internet.

I believe we should explore whether another solution exists, one that aims to respect both the need to foster continued growth of the electronic marketplace and the need to enforce any rules for the protection of consumer privacy. I hope we could develop a solution that respects this dynamic and diverse Internet industry, a solution that would give the industry appropriate power to establish a code of conduct for its online presence, while providing for a limited and proper government oversight role, which, frankly, given the interest received to date in Congress, appears inevitable. This solution possibly could be based on the self-regulatory, quasi-governmental model successfully employed in the securities industry.

Now, I know that can bring a chill over anybody's body in just a few seconds, when you look at how bureaucratically over-regulated in some respects the securities industry is. Yet, still, we have probably the most effective securities industry regulations of any nation and of history itself.

As we continue to examine this issue, I invite any interested person or persons to work with me and other members of this committee to develop a reasonable policy for Internet privacy, one that provides adequate privacy protections for consumers, and at the same time allows the industry to regulate itself in a manner that would allow them to bring new innovations to the marketplace. So I am hopeful that we can do that.

Herb, shall we turn to you at this time to represent the minority?

STATEMENT OF HON. HERBERT KOHL, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator KOHL. Thank you, Mr. Chairman. I would like to commend you for holding this hearing today on the very critical issue of privacy, which is enormously important in the information age that we live in. Public worry over privacy is real. A recent survey found that 92 percent of consumers are, "concerned" about threats to their personal privacy, and that is a startling figure.

Today, new technologies, including the Internet, facilitate the free flow of vast quantities of information around the world. The benefit of this technology is both real and tangible. But as with many other things, there is a downside, especially when this technology allows sensitive personal information, such as medical and credit histories, to be collected and often used by third parties.

Not even the local supermarket is insulated from the information age. Nowadays, stores issue cards that can track information regarding customer purchases right at the check-out counter. Granted, these cards are helpful to consumers who want discounts, but they are not so convenient when the cashier notifies folks in the check-out line that you need to refill your prescription of Prozac.

In much the same way, the Internet can track and store personal data and preferences, oftentimes without the consumer even knowing it. When this information is then shopped around for a profit, privacy is lost and the problems begin.

Certainly, self-regulation is preferable to government regulation, and many in the computer industry have made important strides in this direction. However, striking the right balance between access to information and protection of personal privacy is a complicated matter. While these hearings will help, it is not clear that Congress is equipped to look at this issue with the sort of altitude or distance necessary to resolve these issues. Nor is it clear that the best actors in the private sector will set the standards for the worst.

So, Mr. Chairman, to my mind the time has come to step back and assess privacy concerns from a broader perspective. With Senator DeWine, I am considering legislation to create a privacy study commission which would provide us with a comprehensive overview of the privacy issues we need to focus on today and suggestions of how to ensure privacy tomorrow.

This is not a new idea. In fact, 25 years ago a Privacy Study Commission was established by the Privacy Act of 1974. The work of that commission is legendary. It led to laws protecting financial privacy and credit reporting. But times and technology have changed. In light of the new privacy challenges facing us today and into the next century, which are of a vastly greater magnitude, we need to once again consider a commission approach.

That said, Mr. Chairman, I applaud you and Senator Leahy for holding this important hearing, and I look forward to working with you in the future to address the real privacy concerns of all Americans.

Thank you.

The CHAIRMAN. Well, thank you, Senator Kohl. We appreciate it.

[The prepared statement of Senator Kohl follows:]

PREPARED STATEMENT OF SENATOR HERBERT KOHL

Thank you Mr. Chairman. I would like to commend you for holding this hearing today on the very critical issue of privacy—which is enormously important in the "information age" of today. Public worry over privacy is real. A recent survey found that 92 percent of consumers are "concerned" about threats to their personal privacy—that's a startling figure. Another poll reported that 83 percent believe they no longer have control over how companies collect and use their personal information. No wonder that privacy has caught our attention.

Today, new technologies, including the Internet, facilitate the free flow of vast quantities of information around the world. We've heard time and time again about

the benefits of this "Internet Revolution," and these benefits are both real and tangible. But, as with many things, there is a downside. For example, newer and faster computers make it easier than ever to retrieve medical information in an emergency; but, this technology also allows potentially sensitive personal information, such as medical and credit histories, to be collected and *often* used by third parties.

Not even the local supermarket is insulated from the information age. Nowadays, stores issue cards that can track information regarding customer purchases right at the checkout counter. Granted, these cards are helpful to consumers who want discounts. But they are not so convenient when the cashier notifies folks in the checkout line that you need to refill your prescription for Prozac. [*LAUGHTER*]

In much the same way, the Internet can track and store personal data and preferences, oftentimes without the consumer even knowing it. When this information is then shopped around for a profit, *privacy is lost* and the problems begin.

These are just some of the privacy concerns of Americans, and they are not without consequence. Suspicions regarding Internet privacy, or the lack thereof, have limited the growth of electronic commerce. Many consumers hesitate to participate in on-line activities for fear of having their personal data tracked and stored by unknown parties. There is also the very real problem of harmonizing our privacy laws with the generally stricter—and often less thoughtful—privacy laws of other nations, most notably, the European Union.

Certainly, self-regulation is preferable to government regulation, and many in the computer industry have made important strides in this direction. However, striking the *right balance* between access to information and protection of personal privacy is a complicated matter. While these hearings will help, it is not clear that Congress is equipped to look at this issue with a sort of "altitude" or "distance" necessary to resolve these issues. Nor is it clear to me that the best actors in the private sector will set the standards for the worst.

So Mr. Chairman, to my mind the time has come to step back and assess privacy concerns from a broader perspective. With Senator DeWine, I am considering legislation to create a Privacy Study Commission, which would provide us with a comprehensive overview of the privacy issues we need to focus on today, and suggestions of how to ensure privacy tomorrow.

This is not a new idea. In fact, twenty-five years ago a Privacy Study Commission was established by the Privacy Act of 1974. The work of that Commission is legendary—it led to laws protecting financial privacy and credit reporting. But times and technology have changed. In light of the new privacy challenges facing us today and into the next century—which are of a vastly greater magnitude—we need to once again consider a Commission approach.

That said Mr. Chairman, I applaud you and Senator Leahy for holding this important hearing, and I look forward to working with all of you in the future to address the very real privacy concerns of all Americans. Thank you.

The CHAIRMAN. Senator Leahy is going to be here. So when he arrives, I will probably interrupt to permit him to make whatever statement he desires.

In order to achieve today's dual goal of educating the public and the members of this committee on Internet privacy issues, we are fortunate to have with us six experts in the field of Internet privacy and technology who will testify today.

We will first hear from Ms. Katherine Borsecnik, Senior Vice President of Strategic Businesses at America Online. Ms. Borsecnik has been with AOL for more than 7 years and has played an integral role in developing and implementing AOL's online privacy and safety policies. We are delighted to have you here.

Then we will hear from Mr. Michael Sheridan, Vice President for Strategic Businesses at Novell, headquartered in my home State of Utah. Prior to joining Novell, Mr. Sheridan previously worked at Sun Microsystems, where he was co-creator of the computer programming language Java. Mr. Sheridan is one of the developers of Novell's recently announced digitalme technology.

Are you living in Utah, Michael, or are you down in California?

Mr. SHERIDAN. I am actually out here.

The CHAIRMAN. You are out here?

Mr. SHERIDAN. Yes.

The CHAIRMAN. Also testifying today will be Dr. Irving Wladawsky-Berger, General Manager of IBM's Internet Division. Dr. Wladawsky-Berger has been affiliated with IBM since 1970 and is currently in charge of IBM's Internet and network computing strategy, and is referred to at IBM as "Dr. Internet." I am not sure that that is good.

Mr. WLADAWSKY-BERGER. I am not sure either. [Laughter.]

The CHAIRMAN. I would also like to note that Dr. Wladawsky-Berger is a member of the President's Information Technology Advisory Committee, or PITAC.

Then we will hear from Mr. Jerry Berman, Executive Director of the Center for Democracy and Technology. As its mission states, CDT works to promote democratic values and constitutional liberties in the digital age. Mr. Berman has worked tirelessly with free speech and privacy policy working groups focusing on Internet policy issues.

We are certainly glad to have all of you here.

Next, we will hear testimony from Mr. Russell Bodoff, Senior Vice President and Chief Operating Officer of BBBOnLine, an independent subsidiary of the Council of Better Business Bureaus. Mr. Bodoff is in charge of directing and supervising the creation of BBBOnLine's new Privacy Seal Program, which we are very interested to hear more about today.

Our final witness will be Mr. Greg Fischbach, Chairman and CEO of Acclaim Entertainment, which develops and distributes interactive entertainment software for the Internet and home entertainment systems. Mr. Fischbach is also the Vice Chair of the Board of Directors of the Interactive Digital Software Association.

So we are really happy to have you here, Greg, Mr. Bodoff, Mr. Berman, Mr. Wladawsky-Berger, Mr. Sheridan and Ms. Borsecnik. We think this is a terrific panel and I am looking forward to hearing what you have to say. I would like to thank each of you for taking time out of your busy schedules and appearing before the committee. We expect you, as experts, to shed light on the issues inherent in the protection of privacy on the Internet.

I feel confident that you share my view that Internet privacy issues are too important not to be addressed, and that growth of this new medium and its problems must be addressed carefully. So I have looked forward to today's hearing as a careful and considered first step toward opening a meaningful dialogue between Congress and the interested public on the issue of Internet privacy.

So with that, we will begin with you, Ms. Borsecnik, and we will look forward to hearing what you have to say. I would like you to limit your remarks to five minutes, if you can. I am not going to be a stickler on that, but I would appreciate it if you can because we do have some questions.

PANEL CONSISTING OF KATHERINE BORSECNIK, SENIOR VICE PRESIDENT, STRATEGIC BUSINESSES, AMERICA ONLINE, INC., DULLES, VA; MICHAEL SHERIDAN, VICE PRESIDENT, STRATEGIC BUSINESSES, NOVELL, INC., OREM, UT; IRVING WLADAWSKY-BERGER, GENERAL MANAGER, INTERNET DIVISION, IBM CORP., WASHINGTON, DC; JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC; RUSSELL T. BODOFF, SENIOR VICE PRESIDENT AND CHIEF OPERATING OFFICER, BBBONLINE, INC., ARLINGTON, VA; AND GREGORY FISCHBACH, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, ACCLAIM ENTERTAINMENT, GLEN COVE, NY

STATEMENT OF KATHERINE BORSECNIK

Ms. BORSECNIK. Thank you. I would like to thank you for the opportunity to discuss online privacy with you here today. My name is Katherine Borsecnik. I am Senior Vice President of Strategic Businesses for America Online.

The online medium is quickly revolutionizing the way we learn, communicate and do business. It impacts industries fundamentally as diverse as booksellers to brokerage, and offers consumers unprecedented convenience. Our customers can sign onto AOL and instantaneously do research, send a letter, find the best price on an airline ticket—tasks that just a few short years ago would have taken them far more time.

But the technology of the Internet offers users even something more unique—the ability to customize or personalize their online experience. Consumers can communicate specific preferences online that will allow them to receive services or information that is targeted to their needs. For example, an AOL member can set her online preferences to get the weather forecast in her local area, to read news stories about her professional interests, or to get a notice about the availability of a new CD from her favorite musician.

But the power of the Internet can only be fully realized if consumers feel very confident that their online privacy is protected. For me, protecting my customers' privacy is essential to earning their trust, without which I cannot sustain a business. AOL learned this important lesson through our own mistakes not too long ago when an AOL employee wrongfully disclosed information to the government about a member's screen name.

AOL has recognized that consumer trust is essential to building our business and building the online medium, and we have taken a number of important steps to create a privacy-friendly environment for our customers. Building on the online lessons we have learned, and from the information and opinions we receive from our members on a daily basis, we have adopted privacy policies that clearly explain to our users what information we collect, why we collect it, and how they can exercise choice about how that information is used.

We have based our policies on core principles that reflect consumer needs and expectations. For example, we never read members' private e-mail. We will not disclose to anyone any information about where a member goes online, and we will not give out a

member's phone number, screen name, or credit card information unless he expressly agrees.

We give consumers clear choices about how their personal information is used, and we make sure that our members are well-informed about what those choices are. For example, if a customer decides that he does not want to receive targeted marketing materials from us, all he needs to do is check a box online that tells us not to send him such information.

We also make sure that our policies are well-understood and implemented by our employees. We provide training about our privacy policies and we require all employees to agree to abide by our privacy policies as a condition of their employment at America Online. We continually review state-of-the-art technology to ensure that we use the most advanced technologies to defend our customers' data security.

AOL takes extra steps to protect the safety and privacy of children online. We do not collect personal information from children without their parents' knowledge or consent. We have created a secure environment for children, our Kids Only area, and we carefully monitor all the activity in that area, including chat rooms and message board posts, to ensure the safest possible environment for children, and to ensure that a child does not post personal information online that could allow them to be identified or contacted offline. Furthermore, America Online's parental controls technology enables parents to safeguard their children online by allowing them to set preferences and limits on who their children may talk to online and where they may go and what they may see.

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners and industry colleagues. One of the strongest examples of this effort is our Certified Merchant program, which guarantees that our members will be protected and satisfied when they are within the AOL environment. Through this program, which currently includes over 150 of our merchant partners, we offer a money-back guarantee to dispel consumer concerns about shopping security and increased consumer trust in this powerful new medium.

We believe that the more we are able to work with our business partners and require high standards of them, the more likely it is that these standards will become the marketplace norm. In fact, we believe that the online industry as a whole is taking positive steps toward protecting online privacy. To strengthen industry's commitments to online privacy, AOL joined with other companies and associations last year to form the Online Privacy Alliance, which has grown to include more than 85 recognized industry leaders.

AOL believes that companies are responding to the increasing marketplace demand for online privacy, and that the tremendous growth of e-commerce reflects positive trends on a variety of consumer issues, including privacy. In part, we think that technology holds the key to ensuring a safe and secure online environment. We believe it is critical for us to provide the most sophisticated security technologies to our customers so they can take steps to secure their own privacy. That is why we continue to advocate the widespread availability and use of strong encryption, both in this country and abroad.

Challenges that lie ahead will give us the opportunity to prove that the industry and government can work together to promote effective online privacy. But ultimately for me at the end of the day, it is the consumer who will be the judge of our efforts in these areas and whether they are adequate because no matter how extraordinary the opportunities for electronic commerce are, we know our business will fail if we cannot earn the trust of our customers and meet the consumer demands for privacy protection.

We at AOL are committed to doing our part in this effort. Our consumers demand it, our business demands it, and we appreciate the opportunity to discuss these important issues with you and to work with you further on the issues of Internet electronic commerce and privacy.

Thank you.

The CHAIRMAN. Thank you, Ms. Borsecnik. That was great.

[The prepared statement of Ms. Borsecnik follows:]

PREPARED STATEMENT OF KATHERINE BORSECNIK

Chairman Hatch, Senator Leahy, and Members of the Committee, I would like to thank you, on behalf of America Online, for the opportunity to discuss online privacy with you today. I am the Senior Vice President for Strategic Businesses at AOL, and in that capacity a significant amount of my work for the company is devoted to addressing issues of online privacy, security, and data protection.

The online medium is quickly revolutionizing the way we learn, communicate, and do business. People are migrating to the Internet to meet their commerce and communications needs at an extraordinary rate because it is convenient and fast, and offers an ever-growing selection of information, goods and services. AOL subscribers can sign on to our service and do research, shop for clothes, and buy airline tickets all in a matter of minutes.

In addition, the online environment offers users unique benefits of customization and personalization. Consumers can communicate specific preferences online that will allow them to receive information targeted to their own interests. For instance, AOL members can set their online preferences to get the weather forecast for their own zip code, read news stories about their own hometown, or receive notices about special discounts on their favorite CDs. No other commercial or educational medium has ever afforded such tremendous potential for personalization.

But the power of the Internet can only be fully realized if consumers feel confident that their privacy is properly protected when they take advantage of these benefits. We know very well that if consumers do not feel secure online, they will not engage in online commerce or communication—and without this confidence, our business cannot grow. For AOL, therefore, protecting our members' privacy is essential to earning their trust, and this trust is in turn essential to building the online medium. We learned this important lesson through our own mistakes not too long ago, when an AOL employee wrongly revealed the screen name of one of our members to the government.

Recognizing the importance of this issue, AOL has taken a number of steps to create an environment where our members can be certain that their personal information and their choices regarding the use of that information are being respected: from creating and implementing our own privacy policies and educating our members about them, to promoting best practices among our business partners, to engaging in self-regulatory initiatives and enforcement mechanisms that will raise the bar for all companies who do business online.

SETTING AN EXAMPLE

Building on the lessons we have learned and the input we have received from our members, we have created privacy policies that clearly explain to our users what information we collect, why we collect it, and how they can exercise choice about the use and disclosure of that information. To that end, the AOL privacy policy is organized around 8 core principles:

(1) We do not read your private online communications.

(2) We do not use any information about where you personally go on AOL or the Web, and we do not give it out to others.

(3) We do not give out your telephone number, credit card information or screen names, unless you authorize us to do so. And we give you the opportunity to correct your personal contact and billing information at any time.

(4) We may use information about the kinds of products you buy from AOL to make other marketing offers to you, unless you tell us not to. We do not give out this purchase data to others.

(5) We give you choices about how AOL uses your personal information.

(6) We take extra steps to protect the safety and privacy of children.

(7) We use secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information.

(8) We will keep you informed, clearly and prominently, about what we do with your personal information, and we will advise you if we change our policy.

We give consumers clear choices about how their personal information is used, and we make sure that our users are well informed about what those choices are. For instance, if an AOL subscriber decides that he does not want to receive any targeted marketing notices from us based on his personal information or preferences, he can simply check a box on our service that will let us know not to use his data for this purpose. Because we know this issue is so critically important to our members and users, we make every effort to ensure that our privacy policies are clearly communicated to our customers from the start of their online experience.

We also make sure that our policies are well understood and properly implemented by our employees. We require all employees to sign and agree to abide by our privacy policy, and we provide our managers with training in how to ensure privacy compliance. We are committed to using state-of-the-art technology to ensure that the choices individuals make about their data online are honored.

Finally, we try to keep users informed about the steps they can take to protect their own privacy online. For instance, we emphasize to our members that they must be careful not to give out their personal information unless they specifically know the entity or person with whom they are dealing, and we encourage them to check to see whether the sites they visit on the Web have posted privacy policies.

PROTECTING CHILDREN ONLINE

AOL takes extra steps to protect the safety and privacy of children online. One of our highest priorities has always been to ensure that the children who use our service can enjoy a safe and rewarding online experience, and we believe that privacy is a critical element of children's online safety.

We have created a secure environment just for children—our "Kids Only" area—where extra protections are in place to ensure that our children are in the safest possible environment. In order to safeguard kids' privacy, AOL does not collect personal information from children without their parents' knowledge and consent, and we carefully monitor all of the Kids Only chat rooms and message boards to make sure that a child does not post personal information that could allow a stranger to contact the child offline. Furthermore, through AOL's "parental controls," our members are able to protect their children's privacy by setting strict limits on whom their children may interact with online.

Because of the unique concerns relating to child safety in the online environment, AOL supported legislation in the 105th Congress to set baseline standards for protecting kids' privacy online. We worked with Senator Bryan, the FTC, and key industry and public interest groups to help bring the Child Online Privacy Protection Act (COPPA) to fruition last year. We believe the enactment of this bill was a major step in the ongoing effort to make the Internet safe for children.

FOSTERING BEST PRACTICES

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners and industry colleagues. One of the strongest examples of this effort is our "Certified Merchant" program, through which we work with our business partners to guarantee our members the highest standards of privacy and customer satisfaction when they are within the AOL environment. AOL carefully selects the merchants we allow in the program (currently there are 152 participants), and requires all participants to adhere to strict consumer protection standards and privacy policies. The Certified Merchant principles are posted clearly in all of our online shopping areas, thereby ensuring that both consumers and merchants have notice of the rules involved and the details of the enforcement mechanisms, which help to foster consumer trust and merchant responsiveness.

Here are the criteria that our merchants have to meet in order to become certified and to display the America Online Seal of Approval (some screen shots that show

how these criteria appear to subscribers on our service are attached to this testimony):

1. Post complete details of their Customer Service policies, including: Contact Information, Shipping Information, Returns Policies, and Money-Back Satisfaction Guarantee Information.
2. Receive and respond to e-mails within one business day of receipt.
3. Monitor online store to minimize/eliminate out-of-stock merchandise available.
4. Receive orders electronically to process orders within one business day of receipt.
5. Provide the customer with an order confirmation within one business day of receipt.
6. Deliver all merchandise in professional packaging. All packages should arrive undamaged, well packed, and neat, barring any shipping disasters.
7. Ship the displayed product at the price displayed without substituting.
8. Agree to abide by AOL's privacy policy.

Through our Certified Merchant program, we commit to our members that they will be satisfied with their online experience, and we have developed a money-back guarantee program to dispel consumer concerns about shopping online and increase consumer trust in this powerful new medium. We believe that these high standards for consumer protection and fair information practices will help bolster consumer confidence and encourage our members to engage in electronic commerce.

HELPING TO PROMOTE INDUSTRY EFFORTS

The online industry as a whole is taking positive steps toward protecting consumer privacy. In fact, to improve industry's commitment to online privacy, AOL joined with other companies and associations last year to form the Online Privacy Alliance (OPA), a group dedicated to promoting privacy online.

Since we began our efforts just a few months ago, the OPA has grown to include more than 85 recognized industry leaders, and industry efforts to protect consumer privacy online have blossomed. The OPA has worked hard to develop a set of core privacy principles—centered around the key concepts of notice, choice, data security, and access—and its members are committed to posting and implementing privacy policies that embody these principles. Furthermore, the OPA is continuing to reach out to businesses nationwide to explain the importance of protecting online privacy and posting meaningful privacy policies.

We believe that the OPA member companies are setting a new standard for online privacy, and that as consumers become more aware of the choices available to them, the marketplace will begin to demand robust privacy polices of all companies that do business online. But we also understand the need for meaningful enforcement of self-regulation. That's why we abide by the OPA requirement to participate in robust enforcement mechanisms through our involvement in the TrustE and BBBOnline privacy seal programs. We are key sponsors of both the TrustE and BBBOnline privacy seal programs, and have worked closely with industry representatives and members of the academic community to help formulate strict standards for seal eligibility.

THE CHALLENGES AHEAD

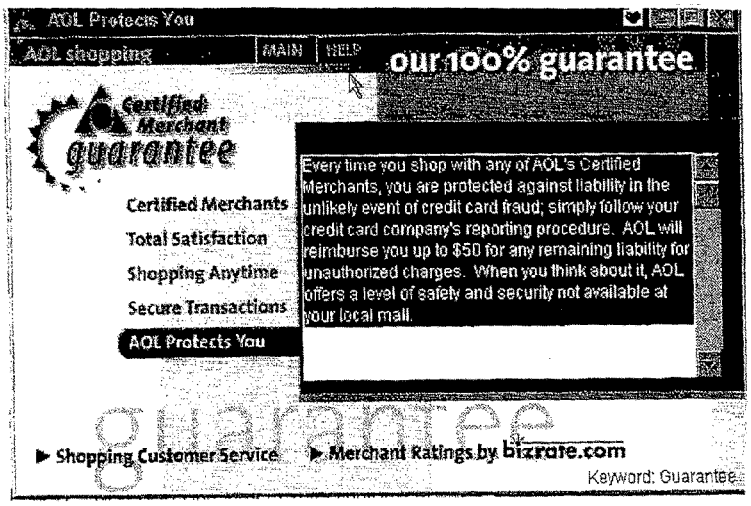
We believe that companies are responding to the increasing marketplace demand for online privacy, and that the tremendous growth of e-commerce reflects positive trends on a variety of consumer protection issues, including privacy. But our work has only just begun. As technology makes it easier for companies to collect and use personal information, the adoption and implementation of robust privacy policies will become even more important.

In part, we believe that technology holds the key to ensuring a safe and secure online environment. As an online service provider, we believe it is critical for us to be able to provide the most sophisticated security technologies to our members so that they can take steps to protect their own privacy online. That's why we will continue to advocate the widespread availability and use of strong encryption, both in this country and abroad.

The challenges that lie ahead will give us the chance to prove that industry and government can work together to promote meaningful self-regulation of online privacy. But ultimately, it is the consumer who will be the judge of whether these efforts are adequate. Because no matter how extraordinary the opportunities for electronic commerce may be, the marketplace will fail if we cannot meet consumers' demands for privacy protection and gain their trust.

We at AOL are committed to doing our part to protecting personal privacy online. Our customers demand it, and our business requires it—but most importantly, the

growth and success of the online medium depend on it. We appreciate the opportunity to discuss these important issues before the Committee, and look forward to continuing to work with you on other matters relating to the Internet and electronic commerce.


AOL Protects You
AOL Shopping
MAIN
HELP
our 100% guarantee
Certified Merchant guarantee
Certified Merchants
Total Satisfaction
Shopping Anytime
Secure Transactions
AOL Protects You
Every time you shop with any of AOL's Certified Merchants, you are protected against liability in the unlikely event of credit card fraud; simply follow your credit card company's reporting procedure. AOL will reimburse you up to $50 for any remaining liability for unauthorized charges. When you think about it, AOL offers a level of safety and security not available at your local mall.
Shopping Customer Service
Merchant Ratings by bizrate.com
Keyword: Guarantee

AMERICA ONLINE CERTIFIED MERCHANTS

Our merchants have been carefully selected because they are able to provide you with the best shopping experience possible. AOL has set a standard for what online customer service should be, and we require that all of our Certified Merchants meet or exceed this high level of service. Here are the criteria that our merchants have to meet in order to become certified and to display the America Online Seal of Approval.

1. Post complete details of their Customer Service policies, including: Contact information, Shipping information, Returns Policies, and Money-Back Satisfaction Guarantee Information.
2. Receive and respond to e-mails within one business day of receipt.
3. Monitor online store to minimize/eliminate out-of-stock merchandise available.
4. Receive orders electronically to process orders within one business day of receipt.
5. Provide the customer with an order confirmation within one business day of receipt.
6. Deliver all merchandise in professional packaging. All packages should arrive undamaged, well-packed, and neat, barring any shipping disasters.
7. Ship the displayed procuct at the price displayed without substituting.
8. AOL's Certified Merchants have agreed to abide by AOL's privacy policy. To read AOL's privacy policy, click here.

We frequently test these Certified Merchants, and are confident that you will enjoy a secure, easy, and fast online shopping experiance.

Happy Shopping Online!

1-800-Baskets
1-800-FLOWERS
911 Gifts
Aardvark Pet Supplies
Access Discount Camera
AKA Gourmet
alle Fine Jewelry
Auction Sales
American Greetings
AOL AutoVantage
AOL Bookshop
AOL Classifieds
AOL Credit Alert
AOL Digital Shop
AOL Hardware Shop
AOL Jean Shop
AOL Modem Shop
AOL Software Shop
AOL Shoppers Advantage
AOL Travelers Advantage
Athletic Shoe Outlet
Audio Book Club
Avon
Balloon Boutique
Barbie Boutique
barnesandnoble.com
Beyond.com
Bid.com
Bluefly
BrainPlay.com
Brooks Brothers
Buy Comp
Campmor
Che's Catalog
Chip Shot Golf
Collectibles Today
Computing Superstore
Cooking.com
Crutchfield
Cybernet Outpost
CyberShop
Digital Chef
Dockers
Eddie Bauer
Egghead.com
EToys
FAO Schwartz
FirstSource.com
frogdog Sports
Fossil Watches
Fragrance Counter
garden.com
Gateway Computers
The Golf Pro Shop
Godiva Chocolatier
Gourmet Marketplace
GreatFoods/Online Specialty Retailing
Hammacher Schlemmer
Health & Vitamin Express
Hickory Farms
iBaby
iQVC
J&R Computer World
JCPenney
Lillian Vernon
Magazine Outlet
Mammoth Golf
Mission Orchards
Mother Nature
Music Boulevard
Netmarket
OfficeMax.com
Omaha Steaks
One Hanes Place
Online Greetings
ONSALE Auction Supersite
Parsons Online
PC Mall
Personal Creations
PetQuarters
Pfaelzer Brothers
Preview Travel
Red Rocket
Reel.com
Seafood Market
Shades.com
Sharper Image
Spiegel
Sports Superstore Online
Total Art
Tower Records
Toys R Us
uBid
ValuPage Brand Coupons
Virtus Vineyards

Since the creation of AOL's shopping area, and the inception of our Guarantee in October 1996, the Shopping Channel has never received a report of a credit card that was compromised during a shopping transaction with Certified Merchants on AOL. This actually makes shopping on AOL safer than at your local mall. Our commitment to our members is to maintain this record by providing you with advanced, up-to-date security technology.

How does AOL make shopping online so safe?

AOL helps to protect you from transaction fraud by making sure that all AOL merchants provide a secure and safe environment for credit card purchases. When making a purchase through AOL, the use of a secure browser scrambles any information that you provide to our Certified Merchants. As a result, in the highly unlikely event that an unauthorized person intercepts the transmission, he/she won't be able to read or to understand any of your personal information. For your convenience and safety, AOL provides you with a secure browser if you are using AOL version 3.0 for Windows, Windows 95, or the Mac (AOL version 2.5 for Windows and 2.7 for Macintosh are not secure browsers). For more information about upgrading your browser, go to Keyword: Browser.

You can protect yourself!

You should also protect yourself from credit card fraud by following this simple guideline: NEVER give your credit card information or password to unauthorized persons contacting you via e-mail or Instant Message. These requests are ALWAYS fraudulent.

AOL, or its affiliates, will NEVER ask you for your credit card number (except during initial AOL registration or when actually making a purchase online) or your AOL password.

For your protection, all AOL Certified Merchants offer return policies that are backed up by AOL's money-back guarantee. If, for any reason, you are not satisfied with your purchase, please contact the merchant through the store's Customer Service area. To view each Certified Merchant's satisfaction guarantee and customer service policies, go to Shopping Customer Service. If, after contacting the merchant, you do not get a satisfactory resolution that is consistent with the store's posted customer service polices, then outline your complaint and notify our Customer Service Help Desk at screen name: MARKETMAIL, and we will intervene on your behalf to assist you in obtaining full satisfaction from the merchant. Should any AOL Certified Merchant not comply with its return policy as stated in the merchant's Customer Service area, then AOL will provide you a refund for the full purchase price. To read more details about Merchant Certification, click the "Certified Merchants" button on the left.

The CHAIRMAN. Mr. Sheridan, before we turn to you, let me turn to our Democrat leader on the committee for his statement. Senator Leahy.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you, Mr. Chairman. As it often happens, I am running between two different committees, and I apologize for going back and forth because this is an area of great interest to me.

I have told this story before. Since I have been in public office, I have clipped and saved and actually framed only about two news items about myself, and I will tell you about one of the two just to give you an idea of why I think this issue is so important.

I live on a dirt road in Vermont. Our nearest neighbors are a mile or so in either direction. One of the neighbors, a farmer, who has known me since I was a teenager, prompted a whole article in the New York Times. An out-of-State car with New York plates pulls up to the farmer. The reporter says, does Senator Leahy live up this road? The farmer says, are you a relative of his? The man says no. The farmer says, are you a friend of his? The reporter says, well, not really. He says, is he expecting you? The reporter says no. The farmer looks him right in the eye and says, never heard of him. [Laughter.]

And I have often thought that probably reflects as much as anything the sense of privacy we have in Vermont, and so I come to this naturally.

The concern over privacy is reaching an all-time high. In 1978, 64 percent of Americans reported they were very concerned or somewhat concerned about threats to their privacy. As Mr. Berman knows, by 1998 this number had skyrocketed. According to the Center for Social and Legal Research, 88 percent of Americans reported being very or somewhat concerned about threats to their personal privacy. So, Mr. Chairman, I thank you and Senator Kohl and others for having this hearing.

Good privacy policies make good business policies. If you have new technologies—and those on the panel know the new technologies as well as anybody in this country—you know that it brings new opportunities for business and consumers. But it doesn't do any good if consumers hesitate to use a particular technology because they are concerned about what it might do to their privacy. That is why privacy policy is good business policy.

Ensuring that we have adequate privacy laws has a more significant and important role in our democracy than just fostering high-tech businesses. We have to defend online freedom from heavy-handed content regulation. The Communications Decency Act in 1996 which was found unconstitutional—I voted against that because of that.

Stopping efforts to create government censors is critical to allow our First Amendment rights to flourish, but it is not enough. For people to feel comfortable in exercising their First Amendment rights, they have to be able to keep their activities confidential and private. If Big Brother is watching, then First Amendment rights are chilled as if government is censoring it.

We have a long tradition of keeping our identities private. The Federalist Papers, for example, the most important political document written about our Constitution, was authored anonymously initially by James Madison, John Jay and Alexander Hamilton, and published under a pseudonym. The Supreme Court, I believe, said "anonymity is a shield from the tyranny of the majority."

The report that I released last month on Vermont Internet commerce is telling on this point. The strongest obstacle among consumers from shopping and doing business online was their fear of the online security risk. This is important because in my State, a rural State like mine, the commercial potential of the Internet is enormous. We have seen businesses that are using it—we have seen their businesses skyrocket, but it is still held back by people who fear the security risks, right or wrong. That is why promoting the use of encryption is so important, so that businesses and consumers can use this technology to provide the privacy and security they need.

I am going to introduce privacy legislation to ensure that Americans' Fourth Amendment rights to be secure in their persons, houses, papers and effects against unreasonable government searches and seizures are given ample protection in a networked computer environment. In addition, several provisions of the bill will address the concern Americans have about the use of their personally identifiable records and information by businesses, satellite carriers, libraries and book sellers.

Online businesses are engaging in serious efforts to make available to consumers information on privacy policies, and I commend and applaud those efforts. But in our current laws, we don't apply privacy principles in an even-handed manner. Video rental stores and cable operators are subject to privacy laws to protect our rights to keep our viewing habits private, but no protections exist for the books we borrow from the library or buy from a bookstore, or the shows we watch via satellite. We should have more privacy for that. For that matter, we should have more privacy on our medical records, which can be moved all over the country without any restrictions.

Telephone companies and cable operators are subject to legal restrictions on how they may use personally identifiable information about their Internet subscribers, but other Internet and online service providers are not. The E-RIGHTS bill I am introducing would promote a more level playing field in terms of the privacy protections available to Internet users, no matter whether they obtain their Internet access from AOL, their cable company, or their local phone company.

So we have to look at a number of things. When should the FBI be allowed to use cell phones to track a user's movements? Should a Kosovo human rights organization that uses a Web site to correct government misinformation be able to get a domain name without having their names publicly available on a database?

Should we allow Federal prosecutors to act like Special Prosecutor Kenneth Starr did and go on fishing expeditions with subpoenas issued to bookstores to find out what we are reading? That was one of the most chilling things I ever saw, a prosecutor going to a bookstore to find out what I was reading. And this is not George

Orwell; this is the United States of America. I mean, of all of Mr. Starr's excesses, this was as bad a one as any I saw.

Should we protect our choices of reading and viewing materials the same way we protect our choice of videotapes that we rent from our local Blockbuster? You may recall that when a Supreme Court nominee was before this committee, somebody had found out what videos he was renting. And Senator Alan Simpson and I were so outraged by that, we introduced legislation saying you can't go into the video stores to find out what they are renting. That was probably the only thing that stopped Mr. Starr on that. If you maintain your calendar on Yahoo, shouldn't you get the same privacy protections as those who keep their calendars on their desks or in their PCs' hard drive?

So these are some of the questions. Mr. Chairman, I know we have witnesses here, and you have been more than gracious with the time. I will put the whole statement in the record, but these are significant privacy issues—and I suspect that you get people in Utah who are very concerned about their privacy, and every State that is represented here. In the electronic world, we have to be more concerned.

The CHAIRMAN. Thank you, Senator.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK LEAHY

Concern over privacy is reaching an all time high. In 1978, 64 percent of Americans reported that they were "very concerned" or "somewhat concerned" about threats to their personal privacy. By 1998, this number had skyrocketed. According to the Center for Social and Legal Research, 88 percent of Americans reported being "very" or "somewhat concerned" about threats to their personal privacy. I am pleased the Senate Judiciary Committee is taking this concern seriously and beginning an examination of new Internet-related privacy issues.

GOOD PRIVACY POLICIES MAKE GOOD BUSINESS POLICIES

New technologies bring with them new opportunities, both for the businesses that develop and market them, and for consumers. It does not do anyone any good for consumers to hesitate to use any particular technology because they have concerns over privacy. That is why I believe that good privacy policies make good business policies.

PROTECTING PRIVACY PLAYS AN IMPORTANT ROLE IN THE EXERCISE OF FIRST AMENDMENT RIGHTS

Ensuring that we have adequate privacy laws has a more significant and important role in our democracy than just fostering high-tech businesses. We also must defend on-line freedom from heavy-handed content regulation. That was my purpose in voting against the unconstitutional Communications Decency Act that became law in 1996.

Stopping efforts to create government censors is critical to allow our First Amendment rights to flourish, but it is not enough. For people to feel comfortable in exercising their First Amendment rights—by speaking, traveling and associating freely online or in physical space—they must be able to keep their activities confidential and private. When Big Brother is watching, the exercise of First Amendment rights is chilled no less than the threat of a government censor.

It is therefore not surprising that our country has a long and honorable tradition of keeping our identities private when we exercise our First Amendment rights. "The Federalist Papers," which is probably the most important political document ever written about our Constitution, was authored anonymously by James Madison, John Jay and Alexander Hamilton and published under a pseudonym.

Healthy advocacy and debate often rests on the ability of participants to keep their identities private and to act anonymously. Indeed, the Supreme Court has said, "Anonymity is a shield from the tyranny of the majority."

Healthy commerce also depends on satisfying consumers' desire to keep their business affairs private and secure. A report I released last month on Vermont Internet commerce is telling on this point. The strongest obstacle among consumers from shopping and doing business online was their fear of the online security risks. This is why promoting the use of encryption is so important, so that businesses and consumers can use this technology to provide the privacy and security they want and that best suits their needs.

I plan to introduce privacy legislation to ensure that Americans' Fourth Amendment rights to be secure in their persons, houses, papers and effects against unreasonable government searches and seizures are given ample protection in a networked computer environment. In addition, several provisions in the bill will address the concern Americans have about the use of their personally identifiable records and information by businesses, satellite carriers, libraries and book sellers.

INDUSTRY SELF-REGULATION EFFORTS SHOULD BE ENCOURAGED

In contrast to a citizen's relationship with his or her government, consumers have a choice of whether they want to deal or interact with those in the private sector. In my view, this choice should be generally recognized in the law by allowing consumers and businesses in the marketplace to set the terms of their interaction. This is an area where the Congress should tread cautiously before regulating. Online businesses are engaging in serious efforts to make available to consumers information on privacy policies so that consumers are able to make more educated choices on whether they want to deal. I commend and applaud those efforts.

That being said, however, current laws do not apply privacy principles in an even-handed manner. Video rental stores and cable operators are subject to privacy laws to protect our right to keep our viewing habits private, but no protections exist for the books we borrow from the library or buy from a bookstore, or the shows we watch via satellite. I am introducing a bill to provide more uniform privacy protection for both books and videos, no matter the medium of delivery.

Similarly, telephone companies and cable operators are subject to legal restrictions on how they may use personally identifiable information about their Internet subscribers, while other Internet and online service providers are not. The E-RIGHTS bill I am introducing would promote a more level playing field in terms of the privacy protections available to Internet users, no matter whether they obtain their Internet access from AOL, their cable company or their local phone company.

THIS LEGISLATION ADDRESSES A BROAD RANGE OF EMERGING HIGH-TECH PRIVACY ISSUES

For example:

- When should the FBI be allowed to use cell phones to track a user's movements?
- Should Kosovo human rights organizations that use Web sites to correct government misinformation be able to get domain names without having their names publicly available on a database? Should we have the same ability to get an "unlisted" domain name (or Internet address) as we are able to get an "unlisted" phone number?
- Should we allow other federal prosecutors to act like Special Prosecutor Kenneth Starr and go on fishing expeditions with subpoenas issued to bookstores to find out what we are reading? Should we protect our choices of reading and viewing materials the same way we protect our choice of videotapes that we rent from our local Blockbuster?
- Should people who maintain their calendars on Yahoo! get the same privacy protection as those who keep their calendars on their desk or on their PC's hard-drive? Will people avoid certain network services offered by Netscape or new Internet start-ups because they get less privacy protection for the information stored on the network than on their own PC's?

These are all important issues, and I have worked to propose solutions to each of these and to other questions, as well, in the E-RIGHTS bill I am introducing. I invite each of the witnesses and others with interests in these matters to exchange ideas on these topics. There are few matters more important than privacy in maintaining our core democratic values.

The CHAIRMAN. We will turn to you now, Mr. Sheridan. We respect all the things that you have done to cause angst throughout the operating platform community.

STATEMENT OF MICHAEL SHERIDAN

Mr. SHERIDAN. Good.

The CHAIRMAN. Yes, it is good, and we are delighted to have you here.

Senator LEAHY. Good word, "angst."

The CHAIRMAN. Yes. We have had a lot of that expressed here before this committee, by the way.

Mr. SHERIDAN. I can feel it.

The CHAIRMAN. Yes.

Mr. SHERIDAN. Mr. Chairman and members of the committee, good morning, and thank you very much for giving me this opportunity to testify on this important issue.

My name is Mike Sheridan. I am Vice President of Strategic Businesses and a member of the Executive Committee of Novell, Inc., which is the world's largest provider of directory-enabled network software, and which is located in the great State of Utah. Prior to coming to Novell in 1988, I worked at Sun Microsystems, where I was one of the original members of the team that created the Java programming language. I testify before the committee today not as an expert in privacy policy, but as a technologist who is building software products that are relevant to the online privacy debate.

At Novell, we view online privacy as an extension of Internet identity, since it is all about empowering users to make decisions about how much information they want to share and with whom. It will come as no surprise to you that I believe that the first line of defense for online privacy is commercial technology. The genius of Net culture is the immediacy with which it funnels resources to new areas and the furious pace, known as Internet time, at which it develops new products. Several new firms have already been established to address privacy on the Web and are attracting significant amounts of venture capital. To the extent possible, we should let the marketplace address privacy concerns, since it will deliver the fastest, most flexible and most cost-efficient solutions.

The second line of defense is industry self-regulation. Before we regulate the Net, we must let the private sector attempt to develop best practices and industry norms that satisfy consumers' needs. The Online Privacy Alliance, TRUSTe, BBBOnLine and the Platform for Privacy Preferences exemplify this effort. We are making steady progress, as witnessed by the rather dramatic increase in the number of privacy policies posted across the Net. Only after we have given commercial technology and self-regulation a chance to work should we turn to government intervention and regulation, and even then we must be sure that it supports America's leadership of the networked economy and needs of consumers.

The first phase of the Internet was really all about getting connected, and companies like AOL made it easy to do this and led the way. For the past years, we have focused on connecting individuals, schools, government and businesses to the Net. The next phase, which is just beginning, will be about creating and managing digital identities. Novell believes that the best way to build the world of Internet identities is to develop products that let individual users create, manage and secure them. The directory, a sort of network white pages, is at the center of our efforts to do so. Identi-

ties and directories are two sides of the same coin. Identities describe who you are on the Net. Directories process this information so that you can connect to the right people, applications and services.

An example of the new technologies that will allow individual choice to govern individual privacy is a product called digitalme. This product reflects Novell's belief that the best way to resolve privacy concerns is to address the larger identity issue. Digitalme allows users to enter and modify personal data in the directory themselves, and to control who has access to it. In other words, it lets people specify the personal information they want to reveal, if any. By providing such tools that allow users to manage their Internet identity, we can educate them about their online privacy.

Because no one technology or company can guarantee privacy on the Web, Novell is also working to promote industry self-regulation. We are currently in discussion with BBBOnLine and are already a member of the Online Privacy Alliance and a premier sponsor and licensee of TRUSTe. Our privacy policy, which is posted on our Web site, was created in accordance with the guidelines of these two groups, as well as the U.S. Federal Trade Commission and EU Directive on Data Protection.

Mr. Chairman, the privacy debate has at times been difficult for the Internet industry. But it has also been very constructive, since it has helped reveal consumer preferences, industry responsibilities, and the new landscape of e-commerce. We should not cut off this debate by pretending that Internet privacy concerns don't exist. Nor should we pass premature legislation that assumes we know all of the answers.

For now, government should encourage private sector solutions, investigate and prosecute deceptive business practices, and monitor privacy abuses to determine the actual harm to consumers. Only after we are satisfied that the private sector cannot meet consumers' needs through commercial technologies and self-regulation should we consider government intervention.

Thank you very much.

The CHAIRMAN. Thank you, Mr. Sheridan.

[The prepared statement of Mr. Sheridan follows:]

PREPARED STATEMENT OF MICHAEL SHERIDAN

Mr. Chairman and Members of the Committee: I am Mike Sheridan, Vice President for Strategic Businesses and a member of the Executive Committee of Novell, Inc., which is the world's largest provider of directory enabled network software. Prior to joining Novell in 1997, I worked at Sun Microsystems where I was one of the original members of the team that created Java. I testify before the Committee today not as an expert on privacy policy, but as a technologist who is building software products that are relevant to the online privacy debate.

What do we mean by online privacy? At Novell, we view it as an extension of Internet identity. It is about empowering users to make decisions about how much information they wish to share and with whom.

With all the press attention that online privacy is getting has come a chorus of calls for government legislation and regulations. We should exercise great caution in responding to them. We are in the early stages of the next big phase of the Internet—a phase that will focus on the creation and management of digital identities and relationships. It would be a mistake to pass legislation regulating privacy on the Net before we fully understand the commercial products and services that will be available to us in this new environment.

The first line of defense for online privacy is commercial technology. The genius of Net culture is the immediacy with which it funnels talent and resources to new

areas—like protection of personal privacy—and the furious pace at which it develops new products. Entrepreneurs have already established several new firms to address privacy on the web, and they are attracting significant amounts of venture capital. We must allow the market to address privacy concerns to the greatest extent possible since it will deliver solutions that are the most flexible, speedy and cost-efficient.

The second line of defense is industry self-regulation. Before we regulate the Net, we must allow the private sector to attempt to develop best practices and industry norms that satisfy consumers needs. The work of TRUSTe, the Online Privacy Alliance (OPA), BBBOnline and the World Wide Web Consortium's Platform for Privacy Preferences (P3P) exemplify this effort. Only after we have given commercial technology and self-regulation a chance to work should we turn to government intervention, and even then we must be sure that they support America's leadership in the networked economy and the needs of consumers.

In my comments today, I will examine three issues that are central to the privacy debate: (1) The next phase of the Internet; (2) The promise of commercial technology; and (3) The principles for future progress.

1. THE NEXT PHASE OF THE INTERNET: THE IDENTITY WAVE

The Internet began as a Department of Defense research project and for many years was used primarily by scientists at national laboratories and research universities. The first big wave of the Internet occurred in the mid-1990's with the advent of the world wide web and the browser. Suddenly, it was easy to surf the Net, and there was a scramble to connect. Companies like Netscape and AOL led the way. Businesses wanted to connect to improve their communications and productivity. Schools wanted to connect to improve educational opportunities; government at all levels wanted to connect to enhance their operations; and individuals wanted to connect to the new world of digital information. Today, US Internet users number about 80 million. The Internet is having an economic impact that is on the scale of the industrial revolution, and it is occurring much faster.

The connection phase will continue for several years as we build out the infrastructure of the web, but it is about to be supplanted by something else—the identity wave. Now that the problems of getting online, getting a browser and using the Net have been largely overcome, we are faced with massive scale issues. These scale issues are really identity problems. How do I find what I want? How do I control my identity when it is scattered over dozens of different sites? How do I keep track of all my passwords? How do I authenticate my digital relationships? How to manage a system this complex in ways that create trust?

Questions about Internet identity are closely related to privacy, but they are not synonymous. Privacy is only one aspect of this identity, albeit a very important one. The best way to resolve privacy concerns is to address the larger issue of how to manage Internet identities.

The transition from the connection phase of the Internet to the identity phase should carry a red flag for public policymakers. Instead of being well along a road we already know we are moving into unfamiliar terrain. Decentralized decision-making and market solutions will serve us better during this transition than centralized government policy since they can respond more quickly and more flexibly to consumers' needs.

2. THE PROMISE OF COMMERCIAL TECHNOLOGY: DIRECTORIES AND DIGITALME™

Entire new companies are being formed and many technologies are being developed to deal with different aspects of online privacy. I cite Novell's approach, not as a panacea, but to illustrate the innovative ways that industry is beginning to respond. Novell believes that online privacy is an extension of Internet identity and that by addressing the broader issue of identity we can resolve many privacy concerns.

The key to building a world of Internet identities is to develop products that let individual users create, manage and secure them. The directory is at the center of our efforts to do so. A true Internet directory is an integrating layer of software that cuts across operating systems to provide a platform for network services. Without a directory, you cannot find, manage or use your network. Directories are what allow network administrators to keep networks up and ready for the user, regardless of where he is or what device he has.

Perhaps the simplest way to think of directories is to compare them to the white pages of a telephone book. Just as white pages contain the information for telephone identities, directories contain the information for Internet identities. But while the white pages are nothing more than a reference guide, a directory is a dynamic data-

base that makes it easy to manage networks, maintain digital interactions and, ultimately, enable widespread electronic commerce.

Digital identities and network directories are two sides of the same coin. Identities describe who you are on the Net; directories process this information so that you can connect to the right people, applications, services and devices.

Novell recently announced a new identity product called digitalme™ that leverages Novell Directory Services so that consumers and businesses can manage their digital identities. Consumers are looking for secure ways to manage and protect their personal information (such as bookmarks, cookies, preferences, user IDs, credit cards and contact information) since these attributes define what they can do, where they can go, and who they are on the web. Companies are looking for opportunities to differentiate their business by creating secure, personalized services that are beneficial to customers.

digitalme™ has a flexible interface built around digital "cards." These virtual meCards can be customized so that users share different information about themselves with different sites based on their personal preferences. For example, a user may want a card for their favorite airline to hold information about their frequent flyer number, their e-mail address, their telephone number, their business travel patterns and their favorite vacation destinations. Voluntarily providing this information would allow the airline to customize its interactions with the user so that if low fares to the users favorite vacation spot are available, for example, the airline can alert them. The same user would provide an entirely different set of personal information to his bank or local hospital. Since the user knows what information he shares, who he shares it with, and when he shares it, he is in more control of his identity on the Net and more aware of his Internet privacy.

digitalme™ is all about user choice. It is downloaded voluntarily from the Net, and is designed so users can enter only the information that they want to share. If they choose to include highly sensitive information a trusted third-party can hold it for them. It puts users in control. By giving users control of their identities, it allows them to create customized solutions that meet their individual needs.

3. PRINCIPLES FOR FUTURE PROGRESS

Some seem to have already come to the conclusion that prompt government intervention is necessary to address concerns about online privacy. Surveys show the protection of personal privacy is the number-one concern many people have about the Internet. And advocates of this view note that it is easier than ever for businesses to gather digital information about consumers without their knowledge or consent and to use this data to market products, or worse, in discriminatory and invasive ways. There is no doubt that the issue of Internet privacy raises legitimate questions about the rights of web users. To the extent that it leads to the erosion of consumer confidence in the Net, it could even retard the growth of electronic commerce.

Nonetheless, it is too early to make a judgement about the need for privacy legislation. Just like the Internet, our understanding of digital privacy is still evolving. The success of Free-PC shows that many consumers are only too happy to trade their privacy rights given the right incentives. And although Internet identifiers can create an invasion of privacy, they are also what allowed the FBI to find the perpetrator of the Melissa virus and to discover who posted the fraudulent Internet articles that artificially inflated the stock price of Pairgain Technologies.

In order to balance these competing concerns, many companies have created privacy policies that share a common set of guidelines. Among the most important are giving consumers notice before gathering any personal data, disclosing how any information that is collected will be used, and letting users choose to opt out of personal data transfers that are not necessary to complete a transaction.

Novell's policy, which is posted on our web site at *www.novell.com,* was created in accordance with the guidelines set forth by TRUSTe, the Online Privacy Alliance (OPA), the US Federal Trade Commission, and the EU Directive on Data Protection. It consists of the following guidelines:

1. In general, people may visit Novell web sites while remaining anonymous and not revealing any personal information. Novell will at times request basic data—such as name, address and e-mail—in order to respond to visitors queries about our products or services, but we will not contact you with additional marketing information unless you indicate that you want to receive it.
2. Novell will not disclose your personal information for marketing purposes to any third-party company without your consent.
3. Novell will not collect information from people who identify themselves as being younger than 18 years of age.

4. Novell may use cookie technology only to obtain non-personal information from its on-line visitors to improve their on-line experience. If you do not wish to have a cookie set when visiting the Novell web sites, you may alter the settings on your browser to prevent them.

5. Novell will take appropriate steps to respect and protect the information you share with us. Whenever you give Novell sensitive information (e.g., credit card numbers), Novell will take commercially reasonable steps to establish a secure connection with your web browser. Credit card numbers are used only for payment processing and are not retained for marketing purposes.

6. All of the information Novell gathers will be available to you at the Novell Identity web page. From this site you can see what kind of information Novell has collected from your visit to our web site and update the information you have provided us in your personal profile. From this site you can also indicate that you would rather be anonymous and provide no information about yourself or your visit to our web site.

As the debate about Internet privacy evolves, we should look to the following principles to guide our efforts:

1. Rely on market-inspired solutions as much as possible

The private sector still has a lot of work to do, but we should not let the highly publicized privacy problems of the past few months distract us from the real progress that has been made. Many organizations have invested a lot of time, effort and money to create a self-regulatory system in which business takes real steps to protect online privacy. OPA, TRUSTe and BBBOnline have educated industry about the issue. Novell and several other companies have developed technologies that hold promise. AOL has made a huge effort to educate consumers. AT&T has funded studies to better understand consumer demand. And IBM has withheld advertising dollars from sites that do not have privacy policies. As a result of these actions, new products are beginning to emerge and privacy policies are steadily proliferating across the Net. If the government decides to take legislative or regulatory action, it should persist in its role as champion of best commercial practice. The private sector is likely to develop faster, more flexible and more cost-efficient solutions than the government and should be encouraged to do so.

2. Refrain from a one-size-fits-all policy approach

Just as no one technology or company can solve the privacy issue, neither can any one policy. Not all information is equal. Some data—such as medical and financial data, and information about children—is especially sensitive. Other types of data can be quite mundane. Moreover, different users have different privacy preferences. Aggressive legislation that treats privacy as a uniform problem could create more problems than it solves.

3. Keep government intervention consistent with the Internet

Where government involvement is needed, it should support and enforce a predictable, minimalist, transparent and simple legal environment. Government should follow a decentralized, technology-neutral approach to policy that encourages private sector innovation. It should refrain from picking technology winners or implementing policies that undermine America's leadership of the networked economy.

4. Enforce existing laws and self-regulation

The government already has an extensive mandate to protect consumer welfare and should vigilantly enforce laws that prevent deceptive trade practices on the Net. Preventing fraud and false advertising are as essential to consumer confidence and the growth of e-commerce as they are to ordinary commerce.

4. CONCLUSION

Mr. Chairman, the privacy debate has at times been difficult for the Internet industry, but it has also been very constructive since it has helped reveal consumer preferences and the new landscape of e-commerce. Just as importantly, it has highlighted industry responsibilities and made us think hard about the appropriate role for public policy. We should not cut off this debate by pretending that Internet privacy concerns don't exist. Nor should we pass premature legislation that assumes we know all the answers. For now, government's role is to encourage private sector solutions, investigate and prosecute deceptive business practices, and monitor privacy abuses to determine the actual harm to consumers. Only after we are convinced that the private-sector cannot meet consumers needs through commercial products and self-regulation should we consider government intervention.

The CHAIRMAN. Mr. Wladawsky-Berger.

STATEMENT OF IRVING WLADAWSKY-BERGER

Mr. WLADAWSKY-BERGER. Mr. Chairman, Senator Leahy, and members of the committee, thank you for the opportunity to comment on the question of privacy in the emerging digital age. My name is Irving Wladawsky-Berger and I am the General Manager of IBM's Internet Division.

Let me begin by reiterating that all of us, individuals and businesses alike, derive incredible benefit from the free flow of information over the Internet. At any hour, day or night, people can check the status of a shipment, analyze their investment portfolios, or compare prices over a whole universe of suppliers. Likewise, businesses gain efficiencies they could only dream of before the Internet, efficiencies that restrain prices and bring them closer to their customers.

All this requires information, lots of it. So, clearly, it is in everyone's interest that the privacy of information be protected. After all, the consumer's embrace of the Internet and the electronic marketplace it makes possible will only last as long as they try us and all the other participants in that marketplace to respect their privacy.

IBM is no stranger to this issue, and we have been working on privacy issues ever since the 1960's. Not surprisingly, then, in 1997 we adopted a worldwide privacy policy for our thousands of Web pages, and at the same time recognized the need for industry to unite on some basic principles and actions. In fact, we have played key roles in the establishment of the Online Privacy Alliance and the TRUSTe and BBBOnLine Privacy Seal programs. We actively support Call for Action, which is an educational program to educate consumers on what they should look for, for privacy on the Web sites.

Most recently, IBM announced that, effective June 1, we would no longer advertise on United States and Canadian Web sites that did not post privacy policies. And as the second largest advertiser on the Web, our action, we hope, should influence the practices of others. That commitment to privacy, and our experience in making the promise of the Net real for thousands of customers, gives us an excellent vantage point from which to view this issue.

It seems to us at IBM that the key question to be answered at this point is how can our society strike the right balance between the value of a free flow of information and privacy. How can that flow of information be not just free, but fair as well?

In our opinion, a broad new statute is not the answer. The Internet is too global, too instantaneous and too decentralized for a fixed, rigid statute to regulate it. The Net and its related technologies simply change too quickly to be amenable to centralized control. We strongly believe that the best way to strike the balance between the free flow of information on the Net and privacy protection is through market forces, which are invariably the product of consumer preferences.

This self-regulation would ride atop a broad base of consumer protection laws and targeted sectoral regulation. This approach envisions a mix of business involvement and commitment, government support and targeted action, international cooperation among businesses and governments, as well as individual responsibility.

Government should defer to private sector leadership for any number of reasons. Number one, the private sector has many incentives to respect privacy, not the least of which is self-interest. The members of the business community simply have too much to gain from the freest possible flow of information and too much to lose if concerns over privacy limit the growth of the networked economy.

Second, excessive regulation can exclude many small and medium firms from the e-business marketplace. We believe that one of the most important opportunities in electronic commerce is to level the playing field, to allow not just the large companies but the smaller companies to participate. We want e-business to benefit Main Street, not just Wall Street.

Third, private sector self-regulation can adapt and change much more quickly and responsibly than government regulation. Fourth, the Internet and the e-business marketplace are fresh, new phenomena and should be regulated very, very carefully and only with good cause. And, finally, the fifth reason for deferring to market forces is the fact that on the Internet information is borderless and the Web itself decentralized, complicating immeasurably all efforts to impose traditional regulation.

The last few years have seen any number of promising marketplace privacy initiatives, and I believe a lot of progress is being made. As my colleague from AOL said, one of the most promising efforts is the Online Privacy Alliance, a cross-industry group established in 1998 to agree on a basic framework for privacy policies tailored to individual industries.

My written statement goes more into detail about the practices of the Alliance. Let me just very quickly talk about what is it based on. Number one, each company should adopt and implement a privacy and post it at its Web site. Two, each visitor to a site should be informed of what personal information is collected at its site, its use, and whether it will be disclosed to others.

Third, visitors to a site should have a choice in whether information will be disclosed to others. Fourth, the Web site owner should take reasonable steps to keep the information secure. And, fifth, the owner should take reasonable steps to keep data accurate and to provide individuals as much access to their identifiable data as is possible.

Let me just conclude by thanking you for the opportunity to appear before you, and afterwards I will be pleased to answer any questions.

The CHAIRMAN. Thank you very much.

[The prepared statement of Mr. Wladawsky-Berger follows:]

PREPARED STATEMENT OF DR. IRVING WLADAWSKY-BERGER

Mr. Chairman, Senator Leahy, and Members of the Committee, thank you for giving me the opportunity to comment on the question of privacy in the emerging Digital Age.

My name is Irving Wladawsky-Berger and I am the General Manager of IBM's Internet Division. In that capacity I am responsible for IBM's Internet strategy, and for driving its implementation across the company. I am also privileged to serve on the President's Information Technology Advisory Committee.

As you may know, IBM is the largest information technology company in the world, with over $81 billion in 1998 revenue and over 290,000 employees worldwide.

We believe this gives us a unique vantage point from which to comment on privacy in the digital age, working as we do with leaders of large, medium and small companies and with governments worldwide, helping them navigate the historic shift to a networked world, and offering them business solutions in the form of expertise, services and technology.

I. THE VALUE OF INFORMATION IN THE INFORMATION AGE

With every passing day it becomes more certain that the Internet will take its place alongside the other great transformational technologies that first challenged, and then fundamentally changed, the way things are done in this world. But with all respect, let me begin my comments by suggesting that, while technological advances in our industry continue at an amazing pace, it is *information* not *technology,* that is at the heart of this revolution.

Information has never been more important than today, when we are engaged in a fundamental transformation of commerce, education, health care, and government—indeed, just about every institution in society that serves individual Americans either as consumers or citizens. For every business, information has assumed an increasingly strategic role. Information is their competitive advantage. It is what allows them to differentiate themselves from all the others in the marketplace who are trying to serve the public.

Leveraging the Internet and other networks so that businesses can better work for all their constituents is what we in IBM call e-business. Indeed e-business is our key market strategy.

We have worked in the marketplace with many thousands of our customers around the world to help them implement e-business strategies. And, one of the things we have learned in the process is that the more information is available to business, government and other institutions, and the more intelligently it is used, the better the job they do serving their customers, dealing with business partners, and running an effective organization. The cumulative effects of all these improvements are greater convenience for consumers, more satisfied constituents, and lower costs that can be passed on to customers in the form of price reductions.

For example, customer self-service applications let consumers obtain whatever information they need anytime of the day or night, whether it is locating a package they have shipped, analyzing the status of their investments, or getting expert advice about a purchase they are contemplating. Moreover, with the amount of information in the World Wide Web growing at a prodigious rate, businesses are increasingly capable of using automated "personalization" techniques, leading questions based on the customer's known needs and wants, to help consumers better navigate through the growing sea of information.

Similar personalization techniques permit retailers to cement relationships with customers by offering promotions on items shoppers are most likely to want. In fact, the Safeway supermarket chain in the United Kingdom typically gets a remarkable fifty percent-plus response rate to their direct promotions based on this simple premise: offering discounts on items they know customers are likely to buy anyway—and Safeway knows what they are likely to buy because of the information people have entrusted to them.

This same retailer, in devising additional customer loyalty programs, discovered that people hate to write shopping lists and invariably forget certain items. So, in cooperation with our research labs, they are piloting a program in which customers get shopping lists matched to their buying patterns. The lists are downloaded to a portable device the customer picks up as he or she enters the supermarket. This same device scans the items as the customer selects them, thus significantly reducing the time spent checking out.

Health care is an area of enormous promise as well. We are working with practitioners around the world to establish high-security health information networks that connect physicians, laboratories and hospitals. With much more timely health information available, patients can receive faster, more effective treatment, and the significantly lower administrative expenses could help restrain medical costs.

But the real promise of these health care networks is the possibility of subjecting all that information to highly sophisticated supercomputing analysis—what we call Deep Computing, since it is similar to that developed in our research labs for our Deep Blue chess playing application—and developing a truly "intelligent" assistant able to deliver expert medical advice to health care professionals. Such expert assistance could be available over networks to practitioners everywhere, in a famous urban medical center or a small rural practice.

In addition, such sophisticated information analysis can infuse far better forecasting and planning into business processes of all sorts. For example, our research lab-

oratories are working with an airline to apply Deep Computing techniques to the scheduling of crew assignments. That improves not only the airline's efficiency, but working conditions as well by matching assignments as much as possible with the preferences of their flight personnel.

That's a great convenience for the flight crews certainly, but it also saves the airline over $80 million annually, costs that would otherwise find their way into airline fare schedules to be paid by the consumer.

In the final analysis, if the digital age is about anything, it is about using information to empower individuals, be they consumers or citizens.

II. ADDRESSING PRIVACY EXPECTATIONS: IBM'S LONGSTANDING COMMITMENT

Incredible prospects exist for enriching the lives of customers, patients, citizens, or just plain individuals by using their information for their benefit, not for their exploitation. And the opportunity to obtain and use that information constitutes a competitive advantage for business. With all that at stake, it stands to reason that the business community has keen incentive to meet people's privacy needs.

This is why IBM takes people's concern for the privacy of their information very, very seriously. IBM understands that consumers will continue to embrace the Internet, and the electronic marketplace it makes possible, only to the degree that they trust those who use the technology to respect the privacy of their personal information. Equipping consumers with knowledge and choice about how their personal information is used is key to building such confidence and trust.

We strive to lead by example via our own policies and behaviors. And we have done so for three decades—a long term commitment to individual privacy, one that predates, in many ways, the policies of industry and government.

1960's

IBM adopted our first formalized and global privacy policy, on handling of employee data, establishing employee access to their personnel folder, well before the practice became common in the workplace.

1970's and 1980's

We formulated specific guidelines and principles, applicable worldwide, on the handling of employee and other data (such as medical records). We instituted management training to ensure compliance. IBM also participated via business groups in the formulation in 1980 of the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and the Transborder Flow of Personal Data. These Guidelines underlie much of the international community's thinking about privacy protection and IBM supports the spirit and intent of the OECD Guidelines.

1990's

As the decade of the Internet began, it was characterized by much hype and a lot of trial and error, but now by the end of the decade the Net emerged as a new mass medium that is transforming how we work, buy, sell, play and learn. As use of the Internet and other networked technologies grew, the need for IBM to renew and refocus its commitment on *today's* privacy issues became clear.

Therefore, in 1997 we adopted and implemented a worldwide privacy policy for our thousands of web pages operating as part of *ibm.com.* A copy of our corporate privacy policy statement from *www.ibm.com* is attached as an Exhibit. Within IBM, we supported adoption of our Web privacy policy with executive communications and the establishment of a new executive position responsible for our internal privacy practices, reporting to IBM's Chief Information Officer.

And we recognized the need for independent third-party backups to company policies, and thus sponsored the formation and launch of both the TRUSTe and BBBOnline privacy seal programs. We also played a key role in the organization and launch of the cross-industry Online Privacy Alliance, the principles of which I describe below. TRUSTe and BBBOnline are independent non-profit groups that can provide consumer assistance and dispute handling for privacy-related questions, and in the case of BBBOnline can respond to any and all consumer queries or complaints. We backed up our own policy by enrolling in the TRUSTe program last year.

IBM also organized or sponsored a number of customer briefings on the issue. In 1998 alone, for example, we hosted a conference in New York City for over 100 senior executives from various business and government organizations. We hosted Secretary of Commerce Bill Daley for a roundtable with over 30 senior executives. With the Software Publishers Association (now the Software and Information Industry Association) we co-sponsored a series of a dozen workshops on web privacy policies.

Recognizing the needs some businesses will have in this area for expert assistance, we also formed a dedicated consulting team in our IBM Global Services division to guide organizations (large and small) through the process of creating and implementing practices that comply with applicable privacy policies or regulations. This team relies on the concept of a "Privacy Architecture" to help organizations adopt the appropriate mix of policies and technologies to manage the privacy and security commitments they make.

We also supported efforts to educate consumers on how to protect their privacy online, most notably funding an effort by Call for Action, a consumer assistance organization, to publicize its "ABCs of Privacy." I've included a sample sticker pamphlet as an Exhibit, and you can find more of their information on *www.callforaction.org*. To their credit, Circuit City supported Call for Action's efforts during the 1998 Holiday season by allowing the organization to distribute this material through their 500-plus stores in the United States.

And most recently, IBM last month stepped forward and announced that, effective June 1, we would no longer advertise on U.S. and Canadian Web sites that did not post privacy policies. As the second largest advertiser on the Web, we believe that our action will influence the practices of other market players. Attached as an Exhibit is the letter sent by our advertising agency, OgilvyOne, to over 350 Web site owners, informing them of our policy.

III. SPREADING THE ADOPTION OF ONLINE FAIR INFORMATION PRACTICES

The key question before all of us at this point is how our society as a whole—business, government and individuals—will strike the right balance between the free and fair flow of information and the reasonable expectations of privacy. In particular, what is the right balance between legitimate government action and the rewards and sanctions of the marketplace?

IBM, led by our CEO Lou Gerstner, has thought about this question a great deal, drawing on our decades of experience with privacy, technology, and business practices. Frankly, we *want rapid progress* in adoption of "fair information practices" by organizations that handle personal data—so that the e-business marketplace, and consumer acceptance of it—will continue to grow at double-digit rates. We also appreciate that U.S. policy makers and other important stakeholders also want rapid progress—especially since electronic commerce has been recognized as a major economic driver of the U.S. economy's success entering the 21st century.

A new statute is not the answer. It would be relatively easy, I suspect, for some to fall into the trap of thinking that enacting a simple statute that tries to make those who operate on the Internet, through whatever means, "respect privacy." But that would give a false guarantee to our citizens—a single "one size fits all" approach could never really meet their expectations for privacy protection, especially in such a complex and fast moving medium as the Internet.

The Internet presents some special challenges that stem from its wonderful and unique attributes. All at once it is: global, instantaneous, and decentralized. Information flows through many packets in order to get routed to its final destination, relying on a very international distribution system that is by its nature decentralized and under no one's ultimate control. The Net and its related technologies change quickly as well. For example, the Internet2 and Next Generation Internet initiatives, under development now in the United States, will soon make it possible to share richer stores of data, much more quickly than before. New technologies and new online startups are challenging us all with their continual changes and new business models.

We strongly believe, therefore, that given these attributes the best way to strike the balance between information flow and privacy protection on the Net is through private sector leadership—what many call "self-regulation"—built atop a base of broad consumer protection laws and targeted sectoral regulation. In order to succeed, we need a mix of business involvement and commitment; government support and targeted action; international cooperation among businesses and governments; and individual responsibility.

IBM strongly supports such a "layered" approach to privacy protection. Where specific, sectoral concerns are identified and are not adequately addressed by self-regulation, some amount of legislation or regulation may be needed. For example, IBM has for several years supported the enactment of medical records privacy legislation—medical data are among the most sensitive data an individual can share, and for that type of data we support a comprehensive statutory framework.

But with respect to the Internet and electronic commerce generally, we believe that self-regulatory efforts should be given more time to address the reasonable pri-

vacy expectations of consumers. There are a number of reasons to defer to private-sector leadership:

The private sector has many incentives to respect privacy

Frankly, since businesses have so much to gain, and so much to lose, if privacy concerns limit the growth of the networked economy, I believe that the members of the business community need to establish themselves as worthy stewards of privacy. We should be encouraged by business' efforts in the last year or so (which I describe below) and we should also recognize that it takes time to grow any movement.

The great majority of the business community recognizes that its real interests lies in maintaining the trust and confidence of their customers—and therefore it is smart business to respect the privacy of personal information.

A number of high-profile examples from the last few years illustrate my point—ranging from AOL, to Geocities, and to the rapid actions taken by Intel and PC makers (including IBM) to address consumer concerns about privacy implication of the new Pentium III chip.

An appropriate role of government vis a vis the private sector in this context would be for all levels of government to lead by example and adopt fair information practices as much as possible. Recent examples involving the reported sale of drivers' license records are good reminders of the importance of providing individuals with "notice" and "choice" over what is done with information they disclose to others. Clearly, the nature of government's responsibilities carries with it duties to secure public safety and investigate potentially harmful actions—but those investigations ought to be executed within our Constitutional protective framework.

Excessive regulation can deter Main Street and others from joining the e-business marketplace

While we agree that the government has a role in protecting the privacy of its citizens, we worry that a pervasive regulatory regime would be cumbersome and stifling, especially for mid-size and small businesses. We want e-commerce to benefit Main Street as well as Wall Street. We want to make sure that businesses of all sizes, from the largest to the very smallest, participate in the networked economy. And, we worry that excessive regulation, with its increased costs, could exclude many from the opportunity represented by the Internet.

Private-sector self-regulation can adapt and change much more quickly and responsively than government regulation

The genius of our nation's Founders produced a political system in which legislation usually develops deliberately and slowly, while policy makers weigh the concerns of opposing factions and competing interest groups. Self-regulation, on the other hand, has the advantage of speed, and the benefit of being able to adapt more quickly to technological changes and consumer and other expectations.

The core forces driving the Internet and e-businesses, of themselves, enable more flexibility in addressing privacy concerns. Empowering technologies such as the Platform for Privacy Preferences, under development as an industry standard by the World Wide Web Consortium, will continue to put in the hands of consumers the power to control their information. Simple technology-related tools one can use today, such as anonymizers and cookie cutters—while not perfect—can be used by all who want to use them. And finally, new business models are springing up that allow people who freely choose to provide information, to get something of value in return. Do you want a free PC today? Or a coupon for products? You decide.

In my view, the best example of private sector responsiveness is the TRUSTe web privacy program. Just launched in 1997, the program has *already* comprehensively updated its privacy policies and practices in order to be consistent with the fundamental principles espoused by the Online Privacy Alliance—the latest "best practices" in online privacy. A regulatory agency would not have been able to accomplish such significant change in that time frame.

The Internet—and the e-business marketplace—are new phenomena and should be regulated very, very carefully and only with good cause

One school of thought says that a new mass medium has been born when it's used by 50 million people. Radio took nearly 40 years to cross that threshold. TV took 13 years; cable TV, 10 years. *The Internet did it in less than five.* By one very conservative estimate the number of Internet users worldwide will surge to 210 million in 1999. Internet commerce will more than double, to $68

billion in 1999. And spending on online advertising grew to nearly $1.6 billion in 1998, an annual growth rate of 83 percent.

Clearly, the Internet is taking off, but so are self-regulatory efforts. I'll turn to a description of these efforts next, but my point is: the U.S. private sector came together in mid-1998, in consultation with government, to agree on robust self-regulation for online commerce. Barely one short year later, we are seeing encouraging early returns, that should elicit additional support for these efforts from policy makers. IBM urges the Committee to encourage such efforts, while being extremely suspect of imposing additional regulation.

Where additional government involvement is deemed necessary, it should address a specific, identified harm or concern—e.g. so called "identify theft" or the rights of citizens against government seizure of online information. An additional role for government, as called for in the recently issued recommendations of the President's Information Technology Advisory Committee, is to support research on fundamental attitudes and technologies related to privacy.

On the Internet, information flows freely across borders; the decentralized nature of the medium complicates efforts to address privacy via traditional regulation. It also highlights the importance of U.S. government actions

National borders do not reflect the basic fabric of the Internet, where information flows freely across borders. Its distributed, decentralized nature means that traditional regulation will have a hard time succeeding in meeting the expectations of citizens that their data will be protected and keep as private as they specify.

The United States today leads all other nations in our use and development of the Net—I can confirm that personally, based on my dealings with people all over the world. It is clear—based on a number of measures—that we lead in the technology, attitudes and practices that are key to succeeding in the New Economy. Other nations watch what we do in this space, and whatever steps our government takes in regulating Internet-related, activity will be carefully studied and potentially copied. To date, our government's willingness to allow the medium to grow led primarily by market forces and technological advances has been a very important precedent abroad, leading governments that are more inclined to impose pervasive regulation to hesitate and in some instances refrain.

Of course, I do not believe that there is no role for government regulation. But I do believe that the best approach involves careful, tailored legislation that allows maximum time and flexibility for self-regulatory efforts to work.

IV. RESPONDING TO THE SELF-REGULATION CHALLENGE

In line with the U.S. system of private-sector leadership supported by statutory requirements, we are seeing a number of promising initiatives.

A number of industry-specific groups have developed privacy principles and initiatives. In the information technology industry, for example, groups such as the Computer Systems Policy Project, the Information Technology Industry Council, and the Software and Information Industry Association have all adopted privacy principles for their members' use and guidance. Attached as an Exhibit are examples from the CSPP and ITI principles—for example, the CSPP developed a full-page ad for *USA Today* that explained their principles, and mailed the information with a letter from eight CEOs to the Fortune 1000 companies of the United States.

One of the most promising examples of self-regulation, and one which IBM strongly supports, is a cross-industry group that came together in 1998 to agree on what constitutes a basic framework of privacy policies that could be tailored to the needs of individual industries. These eighty-plus companies and major trade groups of the Online Privacy Alliance have created guidelines for privacy policies and an enforcement framework with real teeth that each of the Alliance companies (including IBM) has pledged to implement. In doing so we consulted with privacy experts, government and advocacy groups, and arrived at a framework that received generally positive support. Attached as an Exhibit for the Committee's reference are the Alliance Mission, Members, and Guidelines, also found at *www.privacyalliance.org*.

The basic principles that the Alliance companies support for online commerce are, in abridged form:

1. *Adoption and Implementation of a Privacy Policy*—every Web site should post such a policy statement.

2. *Notice and Disclosure of Information Practices*—the statement should give the Web site visitor notice of what personally identifiable information is col-

lected at the site, the use of that information and whether it will be disclosed to third parties.

3. *Choice/Consent*—over whether information is shared or disclosed to others—the individual generally should have a choice, at least the ability to opt out, about whether information about them is disclosed or used for other purposes.

4. *Data Security*—reasonable steps should be taken to keep data secure from unauthorized users or access.

5. *Data Quality and Appropriate Access*—reasonable steps should be taken to keep data accurate and up-to-date, and as appropriate and feasible access to personally identifiable data should be given to the Web site visitor.

6. *Enforcement of the Guidelines by an Easily Available and Usable Mechanism*—all Alliance companies pledge to employ self-enforcement mechanisms that provide consumers with easily understood and used recourse.

Many Alliance companies are working with "seal programs"—independent third parties like the Better Business Bureau's BBBOnLine, and TRUSTe—that monitor a company's compliance with its privacy policy and confer, as it were, a seal of approval. These seals are not empty standards—both BBBOnline and TRUSTe aim to impose requirements that are consistent with the Online Privacy Alliance's standards.

Industry has made real progress in the last year. According to Media Metrix, the independent Web ratings agency, when someone visits a Web site this month chances are over 90 percent that it will be operating under the guidelines of the Online Privacy Alliance. More data will soon be available about industry's progress, when Georgetown University releases a new survey of Web practices next month. I don't know what all of those data will show, but one thing is clear to me: for the large majority of Web users in the United States visiting commercial web sites, they will click on sites that post privacy policies. And if that's not a good test of the successful start of self-regulation, then what is?

IV. CONCLUSIONS

The "layered" approach that I've advocated in this testimony is nothing new for the United States: Attached as an Exhibit is a White Paper and legal analysis prepared by the Online Privacy Alliance that explains the "layered approach" to protecting data privacy in the United States.

As this White Paper states:

> The layered approach to data privacy protection—in which publicly announced corporate policies and industry codes of conduct are backed by
>
> (a) the enforcement authority of the Federal Trade Commission and state and local agencies;
>
> (b) specific sectoral laws that protect the privacy of particular types of information, enforceable by state and federal agencies; and
>
> (c) private civil actions for injunctive or monetary relief brought by individuals or classes of consumers
>
> —differs from the comprehensive government regulatory schemes typically used in Europe. Notwithstanding the absence of any regulatory agency dedicated to the enforcement of privacy standards, however, the "layered" public-private enforcement approach has a long and successful history in the United States.
>
> For example, many professions that traditionally have been trusted to safeguard the confidentiality of personal data—lawyers, doctors and accountants, for example—abide by self-regulatory codes backed up by government or judicial enforcement mechanisms, and the result has been a high level of protection that has stood the test of time.
>
> The framework of self-regulation in the United States, buttressed by the threat of governmental or private enforcement, has succeeded both in protecting personal information and in affording adequate redress to those individuals whose privacy has been invaded. Accordingly, a layered approach—as adapted to address the unique conditions of the Internet—should achieve a level of data privacy protection online that satisfies the principles of the [European Union Data Privacy] Directive.

Online Privacy Alliance, Legal Framework White Paper at 2 (Nov. 1998).

In an economy as networked, global, and competitive as the one we are building, customers usually can impose sanctions and punish a company much faster and more effectively than government. In a free and competitive marketplace, customers will gravitate toward those brands that provide them the best possible service, and

whose brand they can trust. By the same token, with our free and ever-increasing flow of information, empowered people will quickly realize who they should avoid.

Clearly, the less government obtrudes into the marketplace the greater will be the flow of Web transactions delivering goods and services, health care, government services, financial services * * * indeed everything that depends on trust. And flowing from that will come new opportunities, new businesses, and new jobs in all sectors of the economy.

Privacy is not a cut and dried issue. What is and is not private changes from person to person. For one person the scope of privacy is very narrow, for another very broad. For some people privacy is negotiable and they may be willing to trade information about themselves in return for something of value.

Certainly a pervasive regulatory regime could assure the public that nothing improper would happen to their personal information by making sure that nothing *at all* would happen to their personal information * * * nothing bad certainly but nothing good either.

At the other extreme is the laissez-faire solution which might suffice in a perfect world, but as the Founders knew, human nature is far from perfect. Somewhere between those two poles lies the answer * * * some balance between legitimate government action and the rewards and sanctions of the marketplace.

Frankly, I am inclined to find the balance much closer to the marketplace.

After all the great majority of the business community recognizes that its real interests lie in maintaining the trust and confidence of their customers—and therefore in respecting the privacy of personal information. That's why any government privacy policy should provide maximum latitude for stringent self-regulation * * * the kind of discipline that business is already adopting.

Thank you again for the opportunity to appear before you. I would be pleased to answer any questions you may have.

Privacy

TRUSTe

IBM privacy practices on the Web

Personal information

Business relationships

Cookies

IBM is a member of the TRUSTe program. This statement discloses the privacy practices for the IBM Web site.

TRUSTe is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent. Because this site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed and audited for compliance by TRUSTe. When you visit a Web site displaying the TRUSTe mark, you can expect to be notified of:

- What information is gathered/tracked
- How the information is used
- Who information is shared with

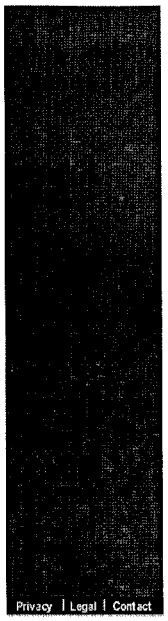
Questions regarding this statement should be directed to the IBM site coordinator (**askibm@vnet.ibm.com**), or **TRUSTe** for clarification. To return to the Site, please use the "Back" button on your browser.

Personal information

At IBM, we intend to give you as much control as possible over your personal information. In general, you can visit IBM on the Web without telling us who you are or revealing any information about yourself. There are times, however, when we may need information from you, such as your name and address. It is our intent to let you know before we collect personal information from you on the Internet.

If you choose to give us personal information via the Internet that we or our business partners may need -- to correspond with you, process an order or provide you with a subscription, for example -- it is our intent to let you know how we will use such information. If you tell us that you do not wish to have this information used as a basis for further contact with you, we will respect your wishes. We do keep track of the domains from which people visit us. We analyze this data for trends and statistics, and then we discard it.

We have implemented these practices for the IBM



Home Page (**www.ibm.com**). We are also instructing our employees around the world to include information on privacy practices everywhere information is collected on the IBM Web, tailored to what that portion of the site does and reflecting the practices outlined here.

Business relationships

The IBM site contains links to other Web sites. IBM is not responsible for the privacy practices or the content of such Web sites.

Cookies

There is a technology called "cookies" which can be used to provide you with tailored information from a Web site. A cookie is an element of data that a Web site can send to your browser, which may then store it on your system. Some IBM pages use cookies so that we can better serve you when you return to our site. You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it. For more information, please see **"How to work with Cookies"**.

IBM is also supporting the development of some technologies that will let you manage and control the release of your personal information wherever you go on the Internet. From time to time we'll be sharing information with you about efforts underway in organizations such as the World Wide Web Consortium and **TRUSTe**.

If you have any questions or comments about our privacy practices, you can contact us at **askibm@vnet.ibm.com**.

OgilvyOne
worldwide

Susan Schiekofer
Senior Partner
Media Director

04/19/99

I am writing to advise you of a new requirement regarding privacy statements that will become part of the U.S. IBM Interactive Advertising Contract.

As I'm sure you are aware, the Internet has become a powerful vehicle for commerce and advertising; for example:

- Internet users will surge 28% to 147 million in 1999
- Internet commerce will more than double, to $68 billion in 1999
- Online advertising grew to nearly $1.6 billion in 1998, an annual growth rate of 83% from the previous year

IBM and OgilvyOne are certainly convinced of the power of the Internet, and have invested considerable resources to advertise in this growing medium.

As research indicates, people are becoming increasingly willing to do e-business. However, there are key elements that will contribute to this growing acceptance. Particularly, that sites and organizations protect:

- the security of transactions
- privacy of personal information

While each of us is eager to protect our customer relationships and private information, recent consumer surveys reveal that good intentions are not enough. People need a visible and understandable reminder that a web site will treat their personal information in appropriate ways.

IBM is among a growing number of companies that have adopted a global privacy policy for its Web sites. Customers can see this policy from a hyperlink on the first screen of the IBM home page.

- IBM's policy is based on principles of self-regulation that are supported by:
  - Leading business-supported organizations in the United States such as the Online Privacy Alliance in the United States (www.privacyalliance.org), TRUSTe (www.TRUSTe.org), BBBOnline (www.bbbonline.org), and FASTforward; and,
  - International policy organizations such as the Organization for Economic Cooperation and Development (OECD)

Therefore, in support of our continued commitment to industry leadership on e-business, effective June 1, 1999, IBM in the United States and Canada will only advertise on Web sites that post a privacy policy statement.

- This spring, the Federal Trade Commission and Georgetown University's Business School will cooperate to release a web survey to gauge the industry's progress in this area. They will profile the numbers of sites posting privacy policies
- We believe that this presents a very timely opportunity for the private sector to continue to take the initiative in posting and following privacy policies.
- While the appropriate privacy statement will vary from site to site, we strongly encourage Web-site owners to employ industry best privacy practices
  - We have surveyed the Web sites that currently carry IBM advertising, and will continue to do so on a regular basis
  - If your site does not currently include a privacy statement, you can refer to www.privacyalliance.org/resources, which provides guidance.

Worldwide Plaza, 309 West 49th Street, New York, New York, 10019-7399, Telephone: (212) 237-6000 Fax: (212) 237-5123 E-Mail: firstname.lastname@ogilvy.com

OgilvyOne
worldwide

We look forward to working with you on behalf of our client IBM to help advance the use of the Internet as a powerful medium where consumers feel secure about the protection of their personal information.

B1 THE WALL STREET JOURNAL WEDNESDAY, MARCH 31, 1999

To Get IBM Ad, Sites Must Post Privacy Policies

By JON G. AUERBACH
Staff Reporter of THE WALL STREET JOURNAL

Big Blue is taking on Big Brother—with a little encouragement from Uncle Sam.

Aiming to allay growing fears about privacy intrusions on the Internet and head off possible government regulation, International Business Machines Corp. has decided to pull its Internet advertising from any Web site in the U.S. or Canada that doesn't post clear privacy policies.

Such policies typically tell Web surfers what information about them is being collected when they visit a site, and how it will be used, sold or otherwise disseminated for marketing purposes. IBM, the No. 2 advertiser on the Internet behind Microsoft Corp., estimates that only about 30% of the 800 sites where it advertises world-wide make such disclosures.

IBM says it will also urge the Internet outlets where it advertises to permit users to opt out of having the information that is collected on them hawked to outside marketers.

The company says it is acting out of both privacy concerns and self-interest, because concerns about privacy are widely regarded as one of the main impediments to wider commercial use of the Internet. The company also hopes to lead a voluntary industry effort to protect privacy on the Web before the government elects to mandate safeguards.

Big Blue plans to announce the move today, and the new policy is scheduled to take effect June 1. Abby F. Kohnstamm, IBM's senior vice president for marketing, says the intent of the new policy is to encourage Internet properties to post privacy guidelines, not to punish the ones that don't.

Although many of the nation's top Internet advertisers have advocated the adoption of privacy policies in recent months, industry officials say IBM is the first large company to specifically link advertising to implementing such policies.

Federal Trade Commission Chairman Robert Pitofsky called IBM's new advertising policy an "admirable step" and said the commission expected other companies to follow. But he added: "If we don't have a level of self-regulation that gives us a sense that there's real progress being made, I think Congress will step in."

The new IBM advertising guidelines come amid growing concerns from individuals about what information is being collected about them and how it is being used. Surveys show potential Internet commerce customers shy away from buying online because of fears that their personal information will be stolen, sold or otherwise compromised. But many Internet sites require users to give registration information, including names and telephone numbers. Some sites also seek credit-card numbers even when purchases aren't being made, ostensibly to allow for later billing.

Despite heightened privacy concerns, relatively few Internet sites have adopted clear-cut privacy policies. In a survey conducted last year, the FTC found that only about 14% of commercial Internet sites disclosed any information about collection practices. The FTC concluded that the level of voluntary adoption of privacy policies on the Internet has "fallen short of what is needed to protect consumers."

Ms. Kohnstamm declined to name advertising sites that haven't posted privacy guidelines. But a search of some of the sites where Big Blue buys ads revealed that Web properties belonging to Andover Advanced Technologies Inc., Times Mirror Co.'s Los Angeles Times, and Bloomberg LP don't include such privacy policies.

A spokesman for the Los Angeles Times says the newspaper plans to post a privacy policy on its Web site in the coming months. Chris Taylor, a spokeswoman for Bloomberg, New York, says the business-news organization intends to add a policy within the next week or so. And Bruce Twickler, president of Andover Advanced Technologies, Acton, Mass., says the Andover.net site it runs doesn't include a privacy policy because the site doesn't sell products or take credit-card information. Mr. Twickler says he intends to post a privacy policy when Andover.net moves into Internet commerce.

IBM plans to spend about $60 million on Web advertising this year, about 10% of its overall ad budget. That's up from $45 million last year, which represented about 7% of IBM's ad spending.

IBM says its Internet advertising agency, OgilvyOne, will send a letter today to alert the approximately 360 sites in the U.S. and Canada where it advertises of the impending changes. OgilvyOne is a unit of Ogilvy & Mather Worldwide. IBM's advertising firm. IBM says it will eventually expand the policy to sites outside North America, especially Asia and Latin America, which IBM says have been lax in observing privacy disclosure.

The letter calls privacy of personal information a "key element that will contribute to the growing acceptance" of conducting business over the Internet. It adds that policy statements are especially important to consumers as a "visible and understandable reminder that a Web site will treat their personal information in appropriate ways."

But some privacy experts say even a clearly stated privacy policy doesn't provide sure privacy. Larry Ponemon, a privacy specialist with PricewaterhouseCoopers LLP in New York, says that companies don't always honor privacy agreements. Even if an Internet user checks a box that requests his information not be sold to direct marketers, "how do you know that the organization is going to honor that and not sell that information?" asks Mr. Ponemon. He also notes that just because an Internet user doesn't disclose his name or address, that doesn't mean that companies can't figure out the user's identity. He points to features built into a new Intel Corp. microprocessor that can tag a request as coming from a specific computer as one way that marketers can establish identities of people on the Internet.

Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington, D.C., argues that privacy disclosure statements simply give Web sites a license to collect and use information however they see fit. "It becomes a privacy policy as a disclaimer," says Mr. Rotenberg, who also teaches at Georgetown University Law School.

IBM says it won't force companies to assure Internet users that their personal information won't be shared. But Ms. Kohnstamm says Web sites should have such features. IBM also suggests that information given by an Internet user should only be used to handle a specific transaction and shouldn't be disseminated without a user's consent.

Such guidelines are also recommended by the Online Privacy Alliance, a coalition of 86 companies and associations that includes IBM, America Online Inc., Compaq Computer Corp., Microsoft and Yahoo! Inc.

PricewaterhouseCoopers estimates that at sites where people are given the choice of opting out of having their information shared, only about 15% choose to do so. But Mr. Ponemon says that percentage is rising as Internet users learn more about the sophistication of direct marketing in cyberspace.

The Electronic Privacy Information Center has pushed for technical changes that would allow people to surf anonymously. The group supports the collection of general demographic information "as long as you don't cross the line of trying to target a known user," says Mr. Rotenberg.

Ms. Kohnstamm says IBM doesn't resell any of the information it gathers on its Internet business sites. In its own privacy statement, IBM says it is "our intent" to let users know how information gathered will be used.

C4 THE NEW YORK TIMES, THURSDAY, APRIL 1, 1999

Advertising | Jeri Clausing

I.B.M. vows to pull ads from Web sites that lack clear policies on protecting consumer privacy.

SAYING it hoped to ward off Government regulation and increase consumer confidence in electronic commerce, the International Business Machines Corporation, the second-biggest advertiser on the Internet, said yesterday that it would pull its ads from Web sites that lacked clear privacy policies.

In a letter sent to 350 Web sites it advertises with in the United States and Canada, **I.B.M.** said that as of June 1 it would advertise only on sites that posted such policies.

The announcement, thought to be the first by a United States company, comes as the Federal Trade Commission, Congress and the European Union are closely monitoring the effectiveness of efforts by on-line businesses to police themselves on the issue of buying and selling personal data they gather.

•

I.B.M. said its own recent survey had found that only 30 percent of the 800 sites worldwide from which it buys ads had privacy policies posted.

"It was a little to our surprise, frankly, that so many sites didn't have privacy policies," said Abby Kohnstamm, I.B.M.'s senior vice president for marketing.

Ms. Kohnstamm and Chris Caine, vice president for governmental programs, cited three factors behind the decision announced yesterday: I.B.M.'s own history of protecting consumer privacy, research showing that consumer concerns about privacy are inhibiting the growth of electronic commerce, and the need for the industry to prove that it can regulate itself.

"Market-led policies need market leaders," Mr. Caine said.

Robert Pitofsky, the trade commission chairman, who last year told Internet companies to make fundamental improvements in protecting consumer privacy or face tough new regulations, said he was encouraged by the announcement.

"I think it is a good move," Mr. Pitofsky said. "I'm not sure whether it will catch on or not, but I think it is important that a company with the stature and prestige of I.B.M. take the first step. Time will tell if others see it in their best interest."

Even privacy advocates who view industry self-regulation as ineffective and unenforceable called the I.B.M. move a positive step in pushing companies to tell consumers what type of personal information they collect and how it is used.

"It is exquisitely timed," said Jason Catlett, president of the Junkbusters Corporation, which promotes consumer protection on line. "I don't think it's going to have an enormous effect," he added, but "I still feel I have to applaud I.B.M. because their heart is in the right place."

Mr. Catlett, saying that I.B.M. had a good history of protecting privacy, also pointed out that the company had avoided negative publicity like that recently faced by the Microsoft Corporation and the Intel Corporation for embedding in their products identifying numbers that could allow marketers and others to track computer users' movements through cyberspace.

All three companies are members of the Online Privacy Alliance, which was formed last year to push companies to address privacy concerns after a survey by the F.T.C. found only 14 percent of Web sites had clear privacy policies posted.

Microsoft, the No. 1 advertiser on the Internet, applauded the move by I.B.M. and said it would watch its effects closely. "Because privacy is very important to us, we are always considering all ways in which we can encourage privacy protections," said Tom Pilla, a Microsoft spokesman. "We don't have any immediate plans to follow suit."

Although I.B.M. will not dictate standards for what privacy policies on Web sites should be, it does refer Web publishers to the Online Privacy Alliance, which has a list of recommended practices that are based on principles recommended by the F.T.C. last year.

The debate over the issue has reached a critical point as the F.T.C. nears a decision on whether a report to Congress due this spring will recommend the passage of new laws to protect on-line privacy.

A group of business interests, in conjunction with the F.T.C. and Georgetown University, recently completed a follow-up to the F.T.C. survey last year of on-line privacy practices. The results of that study, which have not been released, are expected to be a determining factor in the agency's decision.

Mr. Pitofsky told Congress last year that he would push for regulation if significant improvement was not found. He said yesterday that progress was being made, but he acknowledged, "I just don't know how much, and I hear radically different versions from differing groups."

He also emphasized that the report to Congress would look at more than just the numbers. "You want to know what kind of policy" that Web sites "are putting up there," he said. Some key points, he said, are whether the policies are clear and whether they explain that consumers have a choice in how the information they supply is used.

•

Indeed, I.B.M. cited the new survey in the letter that its on-line advertising agency, Ogilvy One Worldwide, a New York unit of **WPP Group** P.L.C., sent out yesterday morning.

"We believe that this presents a very timely opportunity for the private sector to continue to take the initiative in posting and following privacy policies," the letter said in reference to the survey. "While the appropriate privacy statement will vary from site to site, we strongly encourage Web site owners to employ industry best privacy practices."

I.B.M. said it spent about $45 million on on-line advertising last year, or 7 percent of its worldwide media budget. That is expected to increase to $60 million, or 10 percent of its budget, this year.

online privacy alliance

Search our site: Go!

Home | Who We Are | Join | For The Press

Our Mission
Our Members
Privacy Q&A
Privacy News
Resources

for businesses
for consumers
kids privacy

Privacy Policy

Mission

The Online Privacy Alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce.

The Alliance will:

- identify and advance effective online privacy policies across the private sector;
- support and foster the development and use of self-regulatory enforcement mechanisms and activities, as well as user empowerment technology tools, designed to protect individuals' privacy;
- support compliance with and strong enforcement of applicable laws and regulations;
- support and foster the development and use of practices and policies that protect the privacy of children;
- promote broad awareness of and participation in Alliance initiatives by businesses, non-profits, policy makers and consumers; and
- seek input and support for Alliance initiatives from consumer, business, academic, advocacy and other organizations that share its commitment to privacy protection.

Membership Pledge

As members of the Alliance:

- we endorse its mission;
- we commit ourselves to implement online privacy policies consistent with the Alliance's guidelines;

and

- we commit ourselves to participate in effective and appropriate self-regulatory enforcement activities and mechanisms.

webmaster@privacyalliance.org | Privacy Policy | Site Credits | Copyright © 1998 Online Privacy Alliance

online privacy alliance

Who We Are

Online Privacy Alliance Members

The Online Privacy Alliance is a diverse group of more than 80 global corporations and associations who have come together to introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals' privacy online.

If your company or association is interested in joining the Online Privacy Alliance, please let us know.

Member Companies

3Com
Acxiom
AdForce
America Online, Inc.
Ameritech
Apple Computer
AT&T
Bank of America
Bell Atlantic
Bell South
Centraal Corporation
Cisco
CommTouch Software
Compaq
Dell
Disney
Dun & Bradstreet
DoubleClick Inc.
eBay Inc.
Eastman Kodak, Co.
EDS
EDventure Holdings, Inc.
E-LOAN
Engage Technologies Inc.
Equifax
Ernst and Young
Experian
Fast Forward/IAB
Ford

Member Associations

American Advertising Federation
American Electronics Association
American Institute of Certified Public Accountants
Association of Online Professionals
Business Software Alliance
CASIE
(CASIE is representing Association of National Advertisers & American Association of Advertising Agencies)
Computer Systems Policy Project (CSPP)
Council of Growing Companies
Direct Marketing Association
European-American Business Council
Individual Reference Services Group
Information Technology Association of America
Information Technology Industry Council
Interactive Digital Software Association
Interactive Travel Services Association (ITSA)
Internet Alliance
Motion Picture Association of America
Software & Information Industry Association
The United States Council for International Business
The United States Chamber of Commerce

Gateway
GeoCities
Hewlett-Packard
IBM
InsWeb Corporation
INSUREtrust.com LLC
Intel Corp:
Intuit
KPMG
LEXIS-NEXIS
MatchLogic
MCI WorldCom
Microsoft
National Foundation for Consumer Credit
NCR
Nestle' USA
NETCOM On-Line Communication Services, Inc.
Netscape
NORTEL
Novell
northpole.com, LLC
Oracle
Preview Travel
PricewaterhouseCoopers
PrivaSeek, Inc.
Procter & Gamble
Rights Exchange, Inc.
Sun Microsystems
Time Warner Inc.
Unilever United States, Inc.
Viacom
ViewCall Canada, Inc.
Virtual Vineyards
WebConnect
Women.com Networks
Xerox
Yahoo!

---

webmaster@privacyalliance.org | Privacy Policy | Site Credits | Copyright © 1998 Online Privacy Alliance

An open invitation to every company doing business on the Internet.

ONLINE PRIVACY. A TOP PRIORITY FOR US. MAKE IT ONE FOR YOU TOO.

There has been a sea change in the way America does business.

Call it e-commerce, e-business or global electronic commerce. The fact is that the commercial marketplace is a 24-hour-a-day, borderless marketspace—a virtual market for the 21st century.

But as more and more people venture into cyberspace, they are voicing concerns about privacy online.

PEOPLE ARE CONCERNED. WE ARE TOO.

The market for online commerce is expected to reach about $350 billion by 2002.

At the same time, computer users say privacy concerns are the biggest stumbling block to doing more business on the Web.*

The potential for online commerce will only be met if customers trust the companies doing business online.

ONLINE PRIVACY. A TOP PRIORITY FOR CONSUMERS AND BUSINESSES.

That's why we, as some of the leading companies in the information technology industry, have adopted a series of privacy principles to demonstrate our commitment and to promote a new level of consumer trust.

We urge you to adopt them too.

Provide full and clear disclosure on the welcome page of your web site. Consumers have a need and right to know a company's privacy policy before sharing personal information.

It's that simple.

Whatever a company's privacy policy might be, the consumer must be able to see it clearly, and understand it.

Give consumers freedom of choice. Consumers must be able to choose whether they want the information they give to us to be given to others. We must give them the choice, and then respect it.

Take appropriate steps to keep information shared with us secure and accurate. We must help protect our online customers by working to protect their data and providing a means to correct it if needed.

Help protect children online. When Web sites are designed specifically for children, we have a special responsibility to help protect the children who use them by involving their parents, and in most cases, seeking parental consent before any personal information is shared on these sites.

Doing business online means standing shoulder to shoulder with our customers.

It's not just good business sense. It's common sense.

WE URGE YOU TO JOIN US.

Make online privacy a top priority. Adopt and post your own online privacy policy.

Consider joining an organization committed to online privacy, such as the Online Privacy Alliance at www.privacyalliance.org, BBBOnline at www.bbbonline.org, or TRUSTe at www.truste.org.

Help global electronic commerce reach its potential.

For more information about industry efforts to promote online privacy, visit our Web site at www.cspp.org.

CSPP

COMPUTER SYSTEMS POLICY PROJECT

Eckhard Pfeiffer – Compaq Computer Corporation | Michael Dell – Dell Computer Corporation | Louis V. Gerstner, Jr. – IBM Corporation | Lars Nyberg – NCR Corporation

Ronald L. Skates – Data General Corporation | Lewis E. Platt – Hewlett-Packard Company | Andrew S. Grove – Intel Corporation | Lawrence A. Weinbach – Unisys Corporation

COMPUTER SYSTEMS POLICY PROJECT • 1001 G Street, N.W. • Suite 900 East • Washington, D.C. 20001 • 202-393-2260

*According to a recent survey, 65% of Internet users say they are concerned about personal privacy online. But 90% say that the kinds of business actions described here would considerably increase their confidence (Louis Harris Associates/Alan Westin Survey)

Information Technology Industry Council
Rhett Dawson, President
1250 Eye Street, N.W., Suite 200
Washington, D.C. 20005
202/737-8888
Fax: 202/638-4922
www.itic.org

12/97

The Protection of Personal Data in Electronic Commerce

INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Introduction

In the Information Age, advances in information technology (IT), and the corresponding flow of information into the global marketplace are progressing rapidly. These advances provide clear benefits to both society and the individual, including:

- Greater consumer choice and convenience
- Global availability of and access to information
- Increased competition, speed and efficiency

ITI recognizes that appropriate protection and management of personal data is a critical element in enabling consumers to realize the potential of global electronic commerce. (Personal data is defined as any information relating to an identified or identifiable individual.) ITI, which represents suppliers and manufacturers of information technologies, providers of IT services, and collectors and users of personal data, has adopted a policy statement and principles for the protection of personal data in global electronic commerce.

ITI Policy Statement

Collectors and users of personal data, both private and governmental, and the individuals who provide their personal information, share the responsibility for fair and secure use of individually identifiable information. Data collectors and data users should lead by establishing and following effective privacy practices that respond to individuals' reasonable expectations of privacy.

Policies to protect personal data should strike a balance between the societal, economic and individual benefits derived from the free flow of information, and protection of individuals' personal data. Given the rapidly changing developments in technology, this balance can be accomplished primarily by market-led initiatives that provide individuals with technological tools empowering them to enforce their choices to protect their personal data.

Personal data, depending on its nature, varies in the level of sensitivity and need for protection, and market sectors vary in terms of the type of data handled, and how it is handled. Attempts to protect all data equally and without discrimination will limit individual choice, prevent full participation in the global information society, and impose needless complexity and cost. For this reason, industry-by-industry approaches offer the best balance between societal and individual benefits and rights, will result in maximum consumer satisfaction, and are preferable to generic, legislated solutions.

With the advent of information exchange and electronic commerce over the Internet, national and local privacy policies and practices have potentially global effects. Interested parties at all levels must work together to establish reasonable global harmonization of privacy practices to foster the use and the benefits of the global information infrastructure.

ITI Privacy Principles

ITI has adopted these principles for the protection of personal data in electronic commerce for the guidance of ITI members. These principles will serve as a foundation upon which member companies can build their own privacy policies, tailored to their particular business operations.

Information technology companies and on-line service providers, in addition to demonstrating commitment to these principles in their own business practices, should take the lead in making available to consumers the tools and functionalities that enable privacy choices in response to market demand.

These principles reflect the new challenges and opportunities offered by the advent of the global on-line marketplace and ITI's public policy positions.

1. Providing Information on Data Protection Policies.
Collectors and users of personal data should give individuals easily understood information about their policies regarding the collection, use, and disclosure of personal data.

2. Notifying and Empowering the Consumer.
Individuals have the right to be informed about, and exercise reasonable control over, the collection and use of their personal data. ITI member companies are developing market-driven technological solutions enabling individual data providers to exercise choice and control over their personal data. In many cases electronic technologies offer greater personal data protection.

3. Limiting Data Collection.
Collectors and users of personal data should limit the collection of personal data to that which is needed for valid business reasons, and any such data should be obtained by lawful and fair means.

4. Ensuring Data Accuracy.
Collectors and users should strive to maintain the accuracy of the personal data held, including establishing, where appropriate, mechanisms allowing individuals to have the opportunity to review and correct their personal data in defined and secure circumstances.

5. Enabling Informed Choice.
At the time of collection of personal data, collectors and users should furnish individuals with information on the intended use of such data and with mechanisms permitting the exercise of choice on its disclosure.

6. Safeguarding Security.
Collectors and users of personal data should take appropriate steps to ensure that personal data is protected from unauthorized access and disclosure, including limiting access to such data only to those employees with a business need to know.

7. Educating the Marketplace.
Collectors and users of personal data, and particularly IT companies with expertise to share, should support and participate in consumer education efforts about the importance of fair information practices and privacy protection. Individuals should use their powers of choice in the marketplace to safeguard their personal data and that of their children.

8. Adapting Privacy Practices to Electronic and On-line Technologies.
To the maximum extent possible, privacy principles and practices should be the same regardless of the specific technologies employed for data collection and use. Individuals should have a reasonably consistent expectation of privacy in both electronic and paper-based environments.

Members of ITI

AMP Incorporated
Apple Computer, Inc.
AT&T
Bull HN Information Systems Inc.
Compaq Computer Corporation
Dell Computer Corporation
Digital Equipment Corporation
Eastman Kodak Company
Gateway 2000, Inc.
Hewlett-Packard Company
Hitachi Computer Products (America), Inc.
IBM Corporation
Information Handling Services
Intel Corporation
Lexmark International, Inc.
Lucent Technologies, Inc.
Mitsubishi Electric America, Inc.
Motorola, Inc.
NCR Corporation
Panasonic Communications & System Company
Philips Key Modules/USA
Samsung Electronics America, Inc.
Silicon Graphics Inc.
Sony Electronics Inc.
Storage Technology Corporation
Sun Microsystems, Inc.
Symbol Technologies, Inc.
Tandem Computers Incorporated
Tektronix, Inc.
Texas Instruments Incorporated
Xerox Corporation

Are you leaving footprints in Cyber Space

www.this, www.that,
it's everywhere you turn! You can't flip through a magazine, turn on the TV, or listen to the radio these days without hearing an invitation to log on to the Internet. There is, indeed, an abundant, fascinating world waiting to greet you online.

But you've also heard the buzz about *cookies, online security, privacy, passwords,* and *encryption.* So what's a person to do?

Well, before you trek through cyberspace, check out Call For Action's website *(www.callforaction.org).* We'll explain what these buzzwords are all about, and share a few essentials to help you guard your privacy & security online. Get the facts, because a little preparation will go a long way!

As you click your way through the Internet, keep these basic questions in mind to help maintain your online privacy.

STICK THIS ON YOUR MONITOR FOR EASY REFERENCE

Call For Action's **BC's** OF Online Privacy

What information do you collect about me and my family and is it secure?

BENEFITS How do you use that information and what is the benefit to me ?

CHOICES What choices do I have about your use of information about me? Can I opt-out of any information uses and how?

Call For Action Network Office
301.657.8260
Check us out at *www.callforaction.org*

Legal Framework White Paper: Submitted with the Comments of the Online Privacy Alliance On the Draft International Safe Harbor Principles

[November 19, 1998]

OPA WHITE PAPER: ONLINE CONSUMER DATA PRIVACY IN THE UNITED STATES

Introduction

This autumn marks the entry into force of the European Union's Directive 95/46/EC, which establishes minimum requirements for the protection of personal data across the Community and requires member states to prohibit the transfer of personal data to countries where such data is not subject to adequate safeguards. The Directive takes a broad legislative approach to data protection that is not mirrored in federal and state statutes in the United States. Nevertheless, similar concerns about personal privacy in the digital age affect consumer choices, corporate practices, and, ultimately, legal policies—governmental, self-regulatory, and judicial—in the United States. This paper, submitted by the Online Privacy Alliance ("OPA"), illustrates how the collective effect of "layered" regulatory and self-regulatory measures creates "adequate" safeguards for the protection of personal information collected online in the United States.

The OPA is a cross-industry coalition of more than 70 global companies and associations concerned with protecting the privacy of individuals online. As described below, the OPA and its members have adopted standards of conduct tailored to the online environment and intended to ensure that personal information collected online by OPA members receives the level of protection contemplated by the Directive. The OPA has grappled with the unique challenges to and opportunities for data privacy protection that are presented by the enormous and constant data flow in the online environment and has addressed these in a way designed to reflect the realities of the Internet while satisfying the principles of the Directive and U.S. data privacy policies. The OPA has set forth guidelines for online privacy policies, a framework for self-regulatory enforcement, and a special policy concerning collection of information from children. OPA requires its members to adhere to these guidelines and policies, which are available on OPA's website at http://www.privacyalliance.org.

The layered approach to data privacy protection—in which publicly announced corporate policies and industry codes of conduct are backed by (a) the enforcement authority of the Federal Trade Commission and state and local agencies; (b) specific sectoral laws that protect the privacy of particular types of information, enforceable by state and federal agencies; and (c) private civil actions for injunctive or monetary relief brought by individuals or classes of consumers—differs from the comprehensive government regulatory schemes typically used in Europe. Notwithstanding the absence of any regulatory agency dedicated to the enforcement of data privacy standards, however, the "layered" public-private enforcement approach has a long and successful history in the United States. For example, many professions that traditionally have been trusted to safeguard the confidentiality of personal data—lawyers, doctors, and accountants, for example—abide by self-regulatory codes backed up by government or judicial enforcement mechanisms, and the result has been a high level of protection that has stood the test of time. The framework of self-regulation in the United States, buttressed by the threat of governmental or private enforcement, has succeeded both in protecting personal information and in affording adequate redress to those individuals whose privacy has been invaded. Accordingly, a layered approach—as adapted to address the unique conditions of the Internet—should achieve a level of data privacy protection online that satisfies the principles of the Directive.

In recent years the U.S. government has been increasingly concerned about ensuring protection of personal information both online and off. The U.S. government has embraced the layered approach to online data protection and consistently has advocated that self-regulatory efforts—in the form of industry codes of conduct and self-policing trade groups and associations—serve as the primary safeguard to protect the electronic privacy of personal information.[1] This belief in the efficacy of self-regulation reflects U.S. confidence that industry standards will rise to meet the challenge of meaningful data protection, rather than become watered down by a "race to the bottom." Indeed, as discussed below in Part I, the Federal Trade Commission

[1] *See* White House Task Force, *Framework for Global Electronic Commerce* (July 1, 1997).

and the U.S. Department of Commerce have identified five key elements of a successful regime for data privacy protection in order to define for U.S. industry the standards the government expects industry to meet.

(1) *notice* of the ways in which information will be used;
(2) *consent* to the use or third-party distribution of information;
(3) *access* to data collected about oneself;
(4) *security* and accuracy of collected data; and
(5) *enforcement* mechanisms to ensure compliance and obtain redress.[2]

Thus, the U.S. commitment to self-regulation presumes—and will encourage—the development through industry initiatives of *meaningful* privacy measures that generally adhere to these core privacy principles.

The U.S. government, furthermore, has made clear that the failure of a company to abide by privacy standards to which it professes to adhere can subject the company to the enforcement authority of the Federal Trade Commission (or of state and local agencies) and consequent legal penalties. This possibility of government enforcement should provide ample incentives for companies to live up to their guarantees of privacy. *See* Part I *infra.* Moreover, as demonstrated in Part II, both federal and state laws provide an additional layer of privacy protection: They establish numerous types of safeguards for data privacy in various sectors of the economy by imposing legal restrictions on the collection and use of particular types of information. These various laws demonstrate the commitment of both the federal and state governments to intervene and protect privacy if self-regulatory efforts in a particular sector need reinforcement.

The OPA privacy guidelines and attendant enforcement mechanisms (discussed in Part III) are designed to work with this regulatory backdrop to protect the privacy of consumers' online data consistent with the principles set forth in the Directive. OPA-prescribed enforcement mechanisms, such as seal programs, provide a means to guarantee that members comply with clearly identified self-regulatory standards. Companies that identify themselves as adhering to the OPA self-regulatory scheme also may be at risk of FTC (as well as state and local) enforcement actions if they fail to follow the OPA privacy principles; many of these companies also will be obligated to comply with various sectoral data protection laws at the federal and state levels. Thus, compliance with the OPA guidelines should provide assurance to EU data protection authorities that personal information collected online will be adequately protected within the United States, and that such protection is enforceable.

OPA and its members have every incentive to adopt strong standards for data protection and privacy. Political, technological, and economic trends are all driving companies to the high end, not the low end, of privacy protection. Recent polls indicate that public concern about online privacy is the number one reason that consumers not currently using the Internet—still a substantial majority of U.S. consumers—do not go online,[3] and a substantial number of consumers who do use the Internet choose not to purchase goods sold through websites that do not disclose their privacy policies.[4] Congress and the Administration are well aware of the tide of public opinion, and recent events—most notably, the rapid passage by the U.S. Congress of the Children's Online Privacy Protection Act—leave no doubt that the U.S. government will take action if the online industry does not uphold its responsibility to impose meaningful standards for the use and protection of online customer data.

U.S. advocacy of a layered self-regulatory approach to data privacy protection is therefore both a carrot and a stick. Private industry has been given an opportunity to preserve Internet commerce from government regulation—the carrot. However, if self-regulation does not work, or if industry contents itself with meaningless or self-

---

[2] *See Privacy Online* at 7–11 (describing principles in detail); U.S. Department of Commerce, *Privacy and Electronic Commerce* (June 1998); *see also* White House Task Force, *Framedwork for Global Electronic Commerce* (July 1, 1997). The FTC's core privacy principles represent the most recent and comprehensive U.S. effort to identify the fundamental elements of data protection. The FTC framework does not exist in a vacuum, however. The National Telecommunications and Information Agency ("NTIA"), the U.S. Information Infrastructure Task Force, and the Commerce Department each have addressed issues related to the protection of personal information and have all reached similar conclusions as to what constitutes effective data protection. *See Framework for Global Electronic Commerce* (describing results of various studies). The core principles announced by the FTC represent a synthesis of these earlier efforts and the OECD Guidelines. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* 7 & nn. 27, 28 (FTC June 1998), available at http://www.ftc.gov/reports/privacy3.

[3] *See Business Week/Harris Poll: Online Insecurity,* Business Week, Mar. 16, 1998, at 102.

[4] *See* Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web," before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, July 21, 1998; *Privacy Online* at 3–4.

serving standards, the U.S. government stands ready to impose whatever statutory guidelines are necessary for the successful protection of information gathered online—the stick.

This emphasis on meaningful self-regulation has produced real progress in the promulgation of substantive guidelines to govern the use of personal information in certain industries. For example, the major players in the growing market for individual reference services ("IRS")—companies that, for a fee, provide financial and other personal information about individuals—have worked with the Federal Trade Commission to adopt a code of conduct that imposes strict limitations on the use and sale of personal information by those companies. Similarly, the OPA privacy guidelines demonstrate that the self-regulatory framework outlined by the FTC offers a viable method of protecting personal data collected over the Internet.

OPA strongly believes that the interests of its members will best be served by working within that self-regulatory framework to assure the public that personal data will be adequately protected. Online markets are expected to expand dramatically in the coming years, and consumers—particularly those who have yet to buy products or services online—have demonstrated that they in fact care a great deal about the privacy policies of the online companies with whom they do business. New technologies, which will allow a consumer to bargain explicitly for a desired degree of privacy protection, will only heighten public awareness of privacy concerns and reinforce the public's expectation that responsible companies will adhere to the privacy principles espoused by OPA today.[5] Internet markets will not reach their full potential until and unless consumers trust that online businesses will not misuse personal data that must be collected to consummate commercial transactions (e.g., shipping addresses, contact information, credit card numbers). Thus, every commercial online business has an incentive to win that trust by safeguarding the privacy of its customer's personal information, and those forward-looking companies that set the standard for data protection on the Internet—companies like OPA's members—will earn a competitive advantage in the marketplace.

I. THE FEDERAL TRADE COMMISSION: ENFORCING SELF-REGULATION

Private self-regulatory bodies like the OPA—which establish a framework of self-imposed data protection rules to govern the conduct of all entities in a given industry that agree to operate according to those standards—can effectively regulate the behavior of their members and thereby safeguard the private information of consumers. Rather than having to investigate the idiosyncratic information practices of a given company, consumers will learn to associate a prominently displayed seal or notice with a well-known standard of data protection—much as U.S. consumers today know that the "UL" (Underwriters Laboratories) symbol on electronic appliances[6] guarantees that a device's design meets a time-tested safety threshold. Thus, companies that agree to abide by a recognized self-regulatory standard gain the reputational advantage of being able to advertise a consumer-trusted seal of approval—and those that do not bear a stigma that can be expected to affect their performance in the marketplace. Internal enforcement mechanisms guarantee that members live up to their promises by threatening violators with the penalty of losing the organization's stamp of approval.

But the efficacy of collective self-regulation in the United States does not depend on the private sector alone. The Federal Trade Commission ("FTC") may use its enforcement authority under section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive trade practices" in interstate commerce, to prosecute companies that do not uphold the standards of a privacy seal or notice that they display for customers. The FTC has broad jurisdiction over companies doing business in the United States as well as substantial enforcement powers. FTC remedies include injunctive relief and other forms of redress and compensation, and thus impose an independent, objective incentive on companies to take industry standards seriously.[7] State and local consumer protection agencies and consumer advocates, as well as state attorneys general (the latter analogous to the federal Department of

[5] Even today, web browsers can be set to decline "cookies" so as to prevent a website from writing files to a user's disk that permit the site owner to track usage of the website by that user, and filtering programs permit users to prevent access to specified sites, which may include those with unacceptable privacy policies. In the future, automatic protocols like P3P will allow Internet users to negotiate desired levels of privacy protection or to avoid altogether those sites that do not provide sufficient protection for personal information.

[6] The "UL" symbol serves a function similar to the "CE" symbol on products sold in Europe.

[7] *See* Federal Trade Commission, *Individual Reference Services: A Report to Congress* 29 & n.297 (FTC Dec. 1997).

Justice), complement the FTC's authority by keeping a watchful eye on regional industries and smaller businesses.

A. The Federal Trade Commission

1. FTC enforcement authority

The FTC is an independent administrative agency that has been delegated broad enforcement authority under a variety of statutes designed to promote fair competition and protect the interests of consumers. Certain of these statutes—like the Fair Credit Reporting Act (discussed below)—specifically empower the FTC to investigate and prosecute violations of U.S. law governing the treatment of specific types of information relating to an individual's credit and finances. Others—like the recently passed Children's Online Privacy Protection Act of 1998 (also discussed below)—grant the FTC authority to regulate certain data protection practices and dictate minimum standards for the collection and distribution of discrete types of personal information (e.g., data relating to children). More generally, the FTC possesses broad authority under section 5 of the Federal Trade Commission Act to investigate and halt any "unfair or deceptive" conduct in almost *all* industries affecting interstate commerce.[8] This authority includes the right to investigate a company's compliance with its own asserted data privacy protection policies. Pursuant to section 5, the FTC may issue cease and desist orders and may also order other equitable relief, including redress of damages.

While the FTC possesses only limited authority to prescribe regulations that have the force of positive law, it *can* determine (subject to judicial review) that a given practice is unfair or deceptive and therefore contrary to the public interest. Furthermore, if the agency through its adjudicatory procedures determines that a given practice constitutes unfair or deceptive conduct (usually in the form of issuing a "cease and desist order"), other parties who engage in similar conduct are subject to civil penalties if they have actual knowledge of the FTC's determination.[9] Typically, a company will choose not to run the risk of a full-scale FTC investigation and prosecution and will instead enter into a "consent order" with the agency in which a company agrees to comply with objective, judicially enforceable requirements. Thus, the agency often can set a *de facto* minimum standard of behavior through vigorous investigation of companies that engage in questionable conduct, exercising considerable influence over a wide variety of industry practices that the agency deems important to consumers and the public interest. The FTC's recent policy statements and reports leave no doubt that one such area of special concern for the agency is the commercial collection and distribution of personal information.

2. The FTC's core privacy principles

As noted above, in a June 1998 report to Congress, the FTC identified five core principles of privacy protection that it will deem to represent fair and adequate information practices:[10]

> (1) *Notice:* Consumers must be given notice at the time data is collected of (a) what kinds of information are being gathered, (b) whether requests for information may be refused, (c) the uses that will be made of that data, (d) the persons or entities who will receive or have access to that data, (e) the measures taken to ensure confidentiality and accuracy of the data, and (f) whether an individual may limit the dissemination or use of collected personal information.
>
> (2) *Consent:* Individuals should be afforded a choice about the ways in which collected information may be used and whether that information may be distributed to third parties.
>
> (3) *Access:* Individuals should have access to the data that is collected about them and should have some means to correct inaccurate or incomplete information.
>
> (4) *Security:* Companies that collect personal information should take reasonable steps to ensure the *security* and accuracy of that information; in particular, measures should be adopted to prevent unauthorized access to any personal data.

---

[8] Industries exempt from the FTC's enforcement authority under section 5 are in general subject to specific regulatory schemes that tend to be both comprehensive and rigorous. *See, e.g.,* 47 U.S.C. § 45(a)(2) (exempting banks and savings and loan institutions).

[9] *See* 47 U.S.C. § 45(m)(1)(B).

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

(5) *Enforcement:* Individuals must have some mechanism to enforce compliance with an objective code of personal information practices and to obtain redress for violations of that standard.

As demonstrated by the *GeoCities* case (discussed below), the FTC has taken enforcement action to ensure that a company complies with its stated data protection standards.[11] As companies increasingly adopt and announce privacy policies, therefore, their practices become subject to FTC enforcement. Even where a company has not publicly embraced privacy standards, the FTC has cautioned that "in certain circumstances, information practices may be *inherently* deceptive or unfair, regardless of whether the entity has publicly adopted any fair information practice policies," leading to the possibility of an FTC enforcement action under section 5 of the FTC Act.[12] For example, prior to the recent adoption of the Children's Online Privacy Protection Act, the FTC issued an opinion letter concluding that "it is likely to be an unfair practice" to collect personal identifying information from children without a parent's prior consent.[13] As principles of data privacy protection become more ingrained and accepted, other privacy practices similarly could become sufficiently widespread and expected that a company's failure to comply with such practices—at least absent notice to consumers—might be deemed unfair by the FTC.[14]

B. Enforcing Privacy Protection under Section 5 of the FTC Act

A recently settled FTC enforcement action against a website operator demonstrates the FTC's use of section 5 of the FTC Act to assure that companies operate in accordance with their announced information protection practices—thereby putting teeth in self-regulatory programs.[15] This represents the FTC's first resolution of a privacy action in the Internet context by way of a consent order, and illustrates the flexibility of existing U.S. law to adapt to new industry sectors in a timely way.

In the GeoCities case, the FTC challenged the accuracy of certain representations in the website operator's privacy notice regarding the use of marketing information collected from persons registering at the site. The FTC's complaint further alleged that GeoCities implied that it operated a website for children without disclosing to the children or their parents that the website was in fact operated by an independent third party. The company denied these allegations but promptly instituted information policies and procedures in accord with standards proposed by the FTC, as ultimately reflected in a proposed consent order.

Under the terms of the consent order, the company agreed to provide clear and prominent notice to consumers of its actual information practices, including what information is collected through its website, the intended uses for that information, any third parties to whom that information will be disclosed, the means by which a consumer may access information collected from herself or himself, and the means by which a consumer may have that information removed from the company's databases.[16] The company agreed that it would not misrepresent the identity of any

---

[11] *See Privacy Online* at 40 ("[F]ailure to comply with stated information practices may constitute a deceptive practice * * * and the Commission would have authority to pursue the remedies available under the [FTC] Act for such violations.").

[12] *Privacy Online* at 40 (emphasis added).

[13] *See* Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, to Center for Media Education, July 15, 1997, available at http://www.ftc.gov/os/9707/cenmed.htm.

[14] State and local consumer protection agencies also scrutinize the extent to which companies engage in deceptive or misleading practices by failing to adhere to announced codes of conduct, and thus provide additional oversight. *See, e.g.,* Cal. Bus. & Prof. Code §§ 17200, 17500 (West 1998) (revised in 1998 to apply explicitly to Internet commerce); N.Y. Gen. Bus. Law §§ 349, 350 (Consol. 1998); *People* v. *Lipsitz,* 663 N.Y.S.2d 468 (N.Y. Sup. Ct. 1997) (applying N.Y. consumer protection statute to false advertising on Internet); Andrew Countryman, "America Online Deal Reached with 44 Attorneys General," *Chicago Tribune,* May 29, 1998 (describing deal reached between AOL and state attorneys general regarding AOL business practices). In particular, state and local agencies may be better positioned than the FTC to examine the behavior of smaller and regional companies and to respond to the complaints of individual consumers. *See* John Borland, "States Prepare To Examine New Internet Legislation," *CMP TechWIRE,* Jan. 12, 1998 (describing anticipated state legislation to protect Internet consumers). Thus, the enforcement powers and activities of local and state officials and agencies supplements the authority of the FTC and provides an additional layer of protection for personal information.

[15] *See In the Matter of GeoCities,* File No. 9823015 (FTC 1998); *see also* Michael D. Scott, *GeoCities Targeted by FTC in Internet Privacy Enforcement Action,* Cyberspace Lawyer 5–11 (Sept. 1998).

[16] At all points at which information is collected, the company must post either this notice or a link informing consumers that data is being collected and directing them to a complete explanation of the company's information practices.

third party that collects data from a website promoted or sponsored by the company. The company agreed to contact all consumers from whom it previously collected personal information and afford those individuals an opportunity to have data removed from the databases both of the company and any third parties.[17]

Finally, the company agreed to implement procedures to obtain a parent's express consent prior to collecting and using a child's identifying information; moreover, the company may not collect or use a child's identifying information if it has actual knowledge that the child does not have the permission of a parent (or guardian) to disclose that information. The consent order's provisions concerning information gathered from children are virtually identical to those found in the more recently enacted Children's Online Privacy Protection Act.

As a result of this enforcement action, the company must comply on an ongoing basis with the binding rules of conduct specified in the consent order. Beyond that, this highly publicized FTC enforcement action concerning a prominent website operator serves as a benchmark for other companies establishing information practices for their websites.

C. An Industry Model for Facilitating FTC Enforcement of Core Privacy: The IRSG Principles

FTC enforcement is also a powerful tool with respect to enforcement of industry-wide codes of conduct as opposed to company-specific standards or practices. Collective self-regulatory groups can use marketplace dynamics to encourage (or coerce) adherence to a common set of industry "best practices"—no company can afford to be tarred as a recalcitrant that is unconcerned with the privacy concerns of the public (as illustrated on several occasions in recent years when companies withdrew commercial offerings or practices that were publicly criticized as overly intrusive[18]). Moreover, in contrast to the self-regulatory efforts of individual companies, self-regulatory groups can adopt joint mechanisms to investigate and resolve consumer complaints and thus collectively can enforce each company's compliance with a given industry's best practices. FTC oversight—in conjunction with that of state and local authorities—complements such self-regulatory enforcement mechanisms by providing an independent legal incentive for each member company, and the group as a whole, to live up to its promised standard of behavior. The FTC has made clear that, in signing on to an industry group's data protection principles, "a signatory represents that its information practices are consistent with" those principles and that action inconsistent with them subjects a company to liability "under the FTC Act (or similar state statutes) as a deceptive act or practice."[19]

The data privacy standards announced by the Individual Reference Services Group ("IRSG")—an association of fourteen major companies in the individual reference services industry—exemplify a self-regulatory approach emphasizing an industry group's seal of approval. The individual reference services industry gathers personal information about individuals from a number of sources, both public (e.g., state driving records) and private (e.g., credit information) and provides that information for a fee to private parties and the government. To protect the often sensitive personal data with which IRSG members deal on a day-to-day basis, the group has adopted binding standards for the protection of personal information. The IRSG developed these rules with the advice and participation of the FTC, and the agency has endorsed them as a promising mechanism to "lessen the risk that information made available through [individual reference] services is misused * * * [and] address consumers' concerns about the privacy of non-public information in the services' databases."[20] The FTC further recommended that the IRSG's self-regulatory efforts be given an opportunity to demonstrate their effectiveness in conjunction with the FTC's own enforcement activities (and those of sectoral regulatory authorities).[21]

II. SECTORAL REGULATION OF PRIVACY INTERESTS

In addition to the umbrella authority of the FCC over data privacy, the United States has extensive laws regulating the collection and use of consumer data in par-

---

[17] The company agreed as well to cease doing business with any third party that refuses to agree to comply with the data removal provisions of the consent order.

[18] *See, e.g., Individual Reference Services* at 1, 13 & n.1 (describing consumer outrage at Lexis-Nexis's "P-Trak" service, which allowed subscribers to identify an individual's social security number; Lexis quickly changed its policies).

[19] *Id.* at 29 & n.297.

[20] *Id.* at 31.

[21] *See id.*

ticular sectors of the economy. This sectoral approach demonstrates the commitment of the U.S. government—at both the federal and state level—to regulate the privacy of sensitive data and to step in and provide governmental support for self-regulatory regimes.

A. Principal Federal Statutes

1. Fair Credit Reporting Act

One of the primary federal statutes that protects consumer privacy is the Fair Credit Reporting Act ("FCRA"), which regulates the collection and dissemination of a wide range of information about consumers. The purpose of the FCRA, as articulated by Congress, is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information *in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information.*"[22]

In general, the Act regulates the collection and dissemination of "consumer reports," which include information concerning topics such as a consumer's credit worthiness and other personal characteristics, by "consumer reporting agencies"—any person (or entity) who regularly engages in assembling or evaluating these types of information. Such agencies may disseminate consumer report information only to third parties having a specifically delineated permissible purpose for the information, such as a credit transaction or a determination whether to issue an insurance policy. The FCRA also provides further protections, such as the right of consumers to access and obtain correction of data collected and maintained by consumer reporting agencies. On the other hand, the FCRA also provides certain exceptions to its reach, including, for example, situations in which a merchant makes use of data it obtains based on first-hand experience with a consumer.

The scope of the FCRA's privacy protections is dependent primarily on the definitions of "consumer reports" and "consumer reporting agencies." The FCRA defines "consumer reports" broadly to include "any written, oral, or other communication" to a third party of information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part" for one of several general purposes.[23] In particular, information bearing on one of the specified characteristics is a consumer report if it is collected, used, or even expected to be used for purposes including credit, employment, insurance, or a legitimate business need in connection with a business transaction with the consumer.[24] Moreover, the collection or use of the information does not have to be only or even primarily for one of these purposes—it is enough that the information is used, collected, or expected to be used only in part for one of the specified purposes.[25]

This definition of "consumer reports" sweeps a variety of different types of information under the protective umbrella of the FCRA. Data that is collected or used for the purpose of determining credit eligibility or for deciding whether to provide insurance coverage is included.[26] So are reports that are compiled or used to ascertain whether a particular individual is eligible for employment.[27] A list of consumers who have passed bad checks that is supplied to merchants also falls within the category of "consumer reports."[28] The FTC has taken the position that targeted marketing lists also can constitute "consumer reports" within the meaning of the FCRA.[29]

At the same time, the FCRA does provide certain limitations on the definition of a consumer report. As noted above, information does not fall within this category if it is based solely on the disclosing party's first-hand experience with the consumer.[30] Thus, a merchant who discloses the amount and type of its transaction with a consumer is not disseminating a "consumer report" for purposes of the FCRA. This exception may allow dissemination of information without FCRA protection in some circumstances; however, if the recipient of the merchant's firsthand information then sought to pass it on to a third party, the information *would* be protected

---

[22] U.S.C. § 1681(b) (emphasis added).
[23] *Id.* § 1681a(d).
[24] *Id.* §§ 1681a(d), 1681b(a)(3)(F).
[25] *See, e.g., Comeaux* v. *Brown & Williamson Tobacco Co.,* 915 F.2d 1264 (9th Cir. 1990).
[26] FTC Official Staff Commentary, 16 C.F.R. Pt. 600 app. § 603 item 6.
[27] *Id.*
[28] *See Estiverne* v. *Saks Fifth Avenue & JBS,* 9 F.3d 1171 (5th Cir. 1993).
[29] *See Trans Union Corp.* v. *FTC,* 81 F.3d 228 (D.C. Cir. 1996) (noting the FFC's position but remanding for further factual development).
[30] 15 U.S.C. § 1681a(d)(2)(A)(i).

as a consumer report (assuming, of course, that it met the other requirements of the definition).[31] Recent amendments to the FCRA also provide that information communicated to an affiliated entity is not a consumer report if it was "clearly and conspicuously disclosed" to the consumer that such disclosure might occur and the consumer had the opportunity to "opt out" beforehand.[32]

The FCRA generally regulates the collection and dissemination of "consumer reports" only when done by a "consumer reporting agency." The latter term encompasses any person who for money or on a cooperative nonprofit basis "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[33] Examples of consumer reporting agencies include credit bureaus such as Equifax, employment agencies that routinely obtain information on job applicants from former employers, tenant screening companies that assist landlords in checking prospective tenants, and check approval companies that guarantee checks for merchants.[34] On the other hand, an entity that gathers or evaluates consumer data on a one-time or other infrequent basis is not subject to the FCRA.

A consumer reporting agency may legally furnish a consumer report to third parties (in the absence of consent[35]) only if it has reason to believe that the third party has one of the permissible purposes listed in the statute. This generally includes someone who requests information in connection with (1) a credit transaction, review or collection of a credit account, or evaluation of a credit application[36]; (2) a determination whether to issue or cancel an insurance policy or how to set the rates and terms of such a policy[37]; (3) a response to a court order[38]; or (4) a legitimate business need in connection with a business transaction involving the consumer (such as renting an apartment or a consumer's offer to pay by check).[39] In addition, a consumer report may be disclosed to a third party for purposes of an employment decision relating to promotion, reassignment or retention, but only if the consumer authorizes such disclosure in writing beforehand.[40] Marketing is *not* a permissible purpose. The consumer reporting agency must maintain reasonable procedures designed to ensure that consumer reports are furnished only for the listed purposes.[41]

The FCRA also provides further restrictions on the dissemination of "consumer reports." For example, a consumer must consent ahead of time to the release of a consumer report for purposes of employment, credit, or insurance if the report contains medical information.[42] The consumer must have the option to opt out of being included in any lists for unsolicited credit and insurance offers.[43] The FCRA additionally prohibits the reporting of "obsolete information"; the Act sets forth specific time frames after which particular types of data are deemed obsolete.[44]

The Act further mandates that consumer reporting agencies establish "reasonable procedures to assure maximum possible accuracy."[45] The Act seeks to promote accuracy and reliability in part by creating a framework under which a consumer has the right to obtain the information maintained about him or her and require the consumer reporting agency to correct inaccurate information. Specifically, the FCRA requires that every consumer reporting agency disclose upon request to a consumer the "nature and substance" of the information about the consumer in the agency's files, the sources of that information, and the identity of those who have obtained a report about the consumer in the past year.[46] A consumer may dispute the completeness or accuracy of any information maintained by the agency and require the agency to "reinvestigate" the accuracy of the information at no charge to the consumer.[47] The consumer reporting agency generally must complete such reinvestiga-

---

[31] FTC, *Compliance with the Fair Credit Reporting Act* 42 (1977).
[32] 15 U.S.C. § 1681a(d)(2)(A)(iii).
[33] *Id.* § 1681a(f).
[34] FTC Official Staff Commentary, 16 C.F.R. Pt. 600 app. § 603(f) items 4, 6(f).
[35] 15 U.S.C. § 1681b(a)(2).
[36] *Id.* § 1681b(a)(3)(A).
[37] *Id.* § 1681b(a)(3)(C).
[38] *Id.* § 1681b(a)(1).
[39] *Id.* § 1681b(a)(3)(E); FTC Official Staff Commentary, 16 C.F.R. Pt. 600 app. § 604(3)(E) item 3.
[40] 15 U.S.C. §§ 1681b(a)(3)(B), 1681b(b).
[41] 15 U.S.C. § 1681e(a).
[42] *Id.* § 1681b(g).
[43] *Id.* § 1681b(e).
[44] *Id.* § 1681c(a).
[45] *Id.* § 1681e(b).
[46] *Id.* § 1681g(a).
[47] *Id.* § 1681i(a)(1).

tions within 30 days.[48] If the agency concludes that the disputed information is inaccurate or unverifiable, it must modify or delete the information.[49] If, on the other hand, the agency decides that the information is accurate, but the consumer continues to dispute that conclusion, the agency must include the consumer's statement of dispute in any subsequent consumer report.[50]

The Act provides a robust enforcement scheme. Consumers can bring civil actions for damages and attorneys fees for negligent or willful violations of the Act.[51] Punitive damages are also available in the case of willful violations.[52] The Act provides for parallel enforcement at the federal level by the FTC, which can bring actions to enjoin further violations and/or to impose civil penalties.[53] Knowing and willful violations of the Act also can lead to criminal penalties, including imprisonment.[54] Finally, most states have analogous credit reporting statutes giving rise to private rights of actions and providing enforcement powers to the state attorney general.[55]

2. Children's Online Privacy Protection Act of 1998

Recently, in response to a study by the FTC concluding that additional regulation was needed to protect the privacy of children, the U.S. Congress enacted the Children's Online Privacy Protection Act of 1998. The Act directs the FTC to promulgate regulations that govern the collection, use, and disclosure of "personal information" obtained online from a child (defined as anyone under the age of 13) by an operator of a commercial website or online service directed to children, as well as any operator with actual knowledge that it is collecting personal information from a child.[56] "Personal information" is defined to include "individually identifiable information," such as a child's name, address, phone number, social security number, e-mail address, or any other "identifier that * * * permits the physical or online contacting of a specific individual."[57] The Act further reaches any other information collected online that is combined with any of the above identifiers.[58] For example, if a website were to assemble a file including a child's name, address, and a list of past purchases, the information about purchases would be deemed subject to the Act.

Congress directed the FTC to promulgate regulations concerning the collection, use, and disclosure of this personal information about children. These regulations must require, *inter alia,* that website and online service providers subject to the Act

> (1) provide notice on the website of what information is collected, how the operator uses the information, and if/when it discloses the information;
>
> (2) obtain verifiable parental consent for the collection, use, or disclosure of such information;
>
> (3) permit a parent to obtain any data his/her child has provided to the operator;
>
> (4) allow the parent to require the operator to delete such data and/or not to collect further data; and
>
> (5) "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[59]

The Act establishes several narrow exceptions to its reach. For example, its requirements do not apply either to information collected from a child online that is used on a one-time basis to respond to a request and is not maintained in retrievable form or to a request for the name of a parent when made for the sole purpose of obtaining consent to collect information about the child.[60] The Act also contains a "safe harbor" provision under which an operator is deemed to comply with the FTC regulations if it follows a set of self-regulatory guidelines approved in advance by the FTC (after an opportunity for the public to comment) as meeting the requirements of the FTC regulations.[61]

A violation of the regulations promulgated by the FTC under the Act is deemed to be a violation of Section 5 of the FTC Act,[62] the penalties for which are described

---

[48] *Id.*
[49] *Id.* § 1681i(a)(5).
[50] *Id.* § 1681i(c).
[51] *Id.* §§ 1681n, 1681o.
[52] *Id.* § 1681n(a)(2).
[53] *Id.* § 1681s.
[54] *Id.* §§ 1681q, 1681r.
[55] *See, e.g.,* Cal Civ. Code § 1785 *et seq.;* Conn. Gen. Stat. 36–432 to 435.
[56] Children's Online Privacy Protection Act of 1998, §§ 1302(l), 1303(b)(1).
[57] *Id.* § 1302(8).
[58] *Id.* § 1302(8)(G).
[59] *Id.* § 1303(b)(1).
[60] *Id.* § 1303(b)(2).
[61] *Id.* § 1304.
[62] *Id.* § 1303(c).

above. Moreover, the Act provides that certain other specified agencies also shall enforce the Act and the FTC regulations against companies that those agencies regulate; for example, the Department of Transportation must enforce the Act with respect to airlines, and the Federal Reserve Board is charged with enforcement against its member banks.[63] In addition to these forms of federal enforcement, the Act authorizes state attorneys general to bring enforcement actions for injunctive and/or monetary relief for any violation of the FTC regulations.[64]

3. Other federal statutes that protect the privacy of consumer information

Numerous other federal statutes also protect the privacy of particular types of information and provide regulatory and/or judicial enforcement mechanisms:

- *Electronic Funds Transfer Act,* 15 U.S.C. § 1693 *et seq.*—This Act requires institutions that provide electronic banking services to inform consumers of the circumstances under which automated bank account information will be disclosed to third parties in the ordinary course of business. The Act is enforced by the Federal Reserve Board, and violations can result in civil and/or criminal penalties.
- *Electronic Communications Privacy Act,* 18 U.S.C. § 2510 *et seq.*—This statute prohibits the unauthorized interception or disclosure of many types of electronic communications, including telephone conversations and electronic mail, although disclosure by one of the parties to the communication is permitted. Violators of this statute are subject to criminal penalties and civil liability.
- *Video Privacy Protection Act,* 18 U.S.C. § 2710—This statute forbids a video rental or sales outlet from disclosing information concerning what tapes a person borrows/buys or releasing other personally-identifiable information. The Act further requires such outlets to provide consumers with the opportunity to opt out from any sale of mailing lists. The Act is enforced through civil liability actions.
- *Telephone Consumer Protection Act of 1991,* 47 U.S.C. § 227—This provision mandates that any company making a telephone sales call first consult its list of those who have elected not to receive such calls. The statute grants the Federal Communications Commission ("FCC") the authority to prescribe regulations necessary to protect residential subscribers' privacy rights. The Act also bans unsolicited fax messages. It is enforced by the FCC and through civil suits that can give rise to substantial penalties.
- *The Cable Communications Policy Act of 1984,* 47 U.S.C. § 551 *et seq.,* as amended by The Cable Television Consumer Protection and Competition Act of 1992—This Act establishes written disclosure requirements regarding the collection and use of personally identifiable information by cable television service providers and prohibits the sharing of such information without prior consent. The Act also provides consumers with the right to access cable company records for purposes of inspection and error correction. The statutory provisions are enforceable through private rights of action for damages.
- *Communications Act,* 47 U.S.C. § 222—This provision requires telecommunications carriers to protect the confidentiality of customer proprietary network information, such as the destinations and numbers of calls made by customers, except as required to provide the customer's telecommunications service or pursuant to customer consent. These requirements are enforced by the FCC.
- *Federal Aviation Act,* 49 U.S.C. § 40101, *et seq.*—Department of Transportation regulations promulgated under authority of this Act generally require airlines to keep passenger manifest information, such as the names and destinations of passengers, confidential and prohibit use of this data for commercial or marketing purposes.[65] These regulations are enforced by the Department of Transportation.
- *Health Insurance Portability and Accountability Act of 1996,* 42 U.S.C. § 1301, *et seq.*—This Act provides that the Secretary of Health and Human Services must promulgate regulations regulating the privacy of individually identifiable health information if Congress itself does not enact legislation on this subject by August 1999. The Secretary has already issued a set of recommendations to Congress that include provisions such as restricting the disclosure of patient identifiable information and providing patients with notice about how such information will be used and to whom it will be disclosed.

---

[63] *Id.* § 1306(b).
[64] *Id.* § 1305.
[65] *See* 14 C.F.R. §§ 243.7, 243.9.

- *Office of Thrift Supervision Policy Statement on Privacy*[66]—This policy statement advises savings associations on how to best protect consumer privacy. Among other things, the statement urges savings associations to provide notice to consumers as to how personal information will be used and in what circumstances such information may be disclosed to third parties.
- *Right to Financial Privacy Act of 1978,* 12 U.S.C. § 3401, *et seq.*—This Act mandates that the federal government present proper legal process or "formal written request" to inspect an individual's financial records kept by a financial institution (including a credit card company) and give simultaneous notice to the consumer to provide him/her with the opportunity to object. Both government agencies and financial institutions that violate this Act are subject to civil court actions.

B. State Law Protection

In addition to sectoral privacy protection at the federal level, states provide both statutory and common law privacy protection with respect to numerous types of data, particularly in the financial and credit sectors. These state laws sometimes complement similar safeguards at the federal level by providing alternative remedies and enforcement schemes. In other cases, the state laws provide protection for types of data that federal laws do not reach.

1. State statutes

A number of states have statutes that generally concern privacy of financial data. Illinois, for example, regulates the circumstances in which a bank may disclose a customer's financial records, including any information "pertaining to any relationship established in the ordinary course of a bank's business."[67] In addition to the state analogues to the FCRA discussed above, a number of state statutes specifically address the use of consumer credit information, particularly for marketing purposes. Maine, for example, generally forbids any sale or disclosure of mailing lists or account information of credit card holders to a third party without an explicit opt-in by the consumer.[68] Florida and Hawaii also have opt-in schemes for dissemination of credit card lists, except that they allow disclosures to a third party as long as that party is prohibited from divulging consumer information except to carry out the purpose for which the cardholder provided the information.[69] California requires that, before a credit card issuer discloses marketing information to any person, the issuer must inform the cardholder of such disclosure by written notice that provides an opportunity to opt out of the program.[70]

State statutes also extend privacy protections to other sectors of the economy. A number of states, for example, restrict the collection and disclosure of information gathered by insurance companies. These statutes, based on the Insurance Information and Privacy Protection Model Act promulgated by the National Association of Insurance Commissioners, often require insurance companies and agents to provide a policyholder or applicant notice concerning the types of personal information that may be collected about him or her from a third party and the individual's rights to access and correct information in the company's files.[71] Many state statutes also protect the privacy of medical information by, for example, providing patients a general right of access to their medical records[72] and protection from disclosure of medical records by licensed health-care providers.[73]

2. State common law

States also provide privacy protection through a number of common law doctrines. On a general level, virtually all states recognize a tort of invasion of privacy. This tort is generally divided into four categories: intrusion upon seclusion of another, appropriation of another's name or likeness, unreasonable publicity given to another's private life, and publicity placing another in a "false light" before the public.[74] The most relevant form of this tort in the context of protecting an individual's private data is giving unreasonable publicity to another's private life. Although this

---

[66] Office of Thrift Supervision, *Statement of Privacy and Accuracy of Personal Customer Information* (Nov. 1998).
[67] Ill. Rev. Stat. ch. 202, § 5/48.1; *see, e.g.,* Minn. Stat. § 13A.01; N.J. Stat. Ann. § 17:16K–3.
[68] Me. Rev. Stat. Ann. tit. 9–A, § 8–304.
[69] Fla. Stat. ch. 817.646; Haw. Rev. Stat. § 708–8105.
[70] Calif. Civ. Code § 1748.12(b).
[71] *See, e.g.,* Cal. Ins. Code § 791; Conn. Gen. Stat. Ann. § 38–501; Ill. Rev. St. ch. 215, § 5/1001.
[72] *See, e.g.,* Cal. Health & Safety Code § 1795; Colo. Rev. Stat. § 25–1–801.
[73] *See, e.g.,* Fla. Stat. chs. 455.241, 395.017.
[74] *Restatement (Second) of Torts* § 652A (1977).

tort is unlikely to apply to the disclosure of arguably public information such as names and addresses, release of more private information such as transaction histories might trigger this tort.[75]

In certain cases, the relationship between the consumer and the holder of consumer data gives rise to a legally cognizable duty not to disclose consumer information or to do so only in particular circumstances. A number of states, for example, have recognized an implied contractual duty on the part of banks not to disclose information about a depositor's account.[76] A similar duty arguably arises in the context of a creditor-debtor relationship[77] and a security firm-customer relationship.[78]

Finally, state regulation of professionals, such as accountants, doctors, lawyers, and psychologists, often impose restrictions on the use and disclosure of personal information such professionals obtain from their clients. Often the state code simply enforces or supports the self-regulatory code adopted by the profession. For example, many states protect communications between doctors and psychiatrists and patients, recognizing those professions' commitment to safeguarding such communications. Some states also have recognized that accountants have a general duty to maintain the confidentiality of client information.[79] State laws often provide additional protections by determining that these professional codes of conduct create fiduciary duties on the part of professionals and permitting civil suits for breach of those duties.

III. THE ONLINE PRIVACY ALLIANCE: USING SELF REGULATION TO SAFEGUARD CONSUMER PRIVACY ONLINE

In keeping with the traditional commitment to self regulation in the United States and in response to the FTC's and the Clinton administration's call for responsible self-enforcement of privacy protection by U.S. industry, many U.S. businesses have come together to begin exploring the creation of self-regulatory programs. One particularly successful example of this effort has been the OPA, which brought together over 70 leading global companies and associations beginning in 1998 to address growing public concern over online privacy issues.

The online medium creates particular challenges for privacy protection while simultaneously creating significant opportunities for consumer privacy education and empowerment. The challenges are manifold: Use of the Internet necessarily involves a tremendous flow of information, much of it personal in nature, in a wide variety of contexts. Some information flows involve the consumer actively providing information. For example, commercial Internet transactions require consumers to provide credit card or other payment and contact information, and in certain more sensitive contexts, some transactions may require other identifying data. Some sites may seek data in order to satisfy the consumer's request for information or services, such as where a consumer is asked about family size or smoking habits in response to an inquiry about hotel accommodations. Other sites may request data simply to use for marketing purposes. Consumers also may provide a great deal of data in order to obtain personalized services, such as targeted clipping services or personalized Internet service offerings. In some cases, consumers provide data without necessarily realizing they are doing so. For example, simply visiting or subscribing to certain online sites or services may itself create a footprint that conveys data about the individual's interests. But regardless of the context, all data collected online is already in digital format, which makes it easy to manipulate, store, and process, and in turn provides massive capabilities for use and transfer of data. Meanwhile, unless effective security measures are used, collection of data online is susceptible to computer "hacking" by unauthorized users, and also to fraud by consumers posing as a third party.

These challenges place a special obligation on the online industry to educate consumers about the Internet's privacy risks and to enhance consumers' ability to make educated choices about how to protect their privacy rights. And indeed, the online medium provides tremendous opportunities for consumer data protection. Online merchants have an unmatched ability to provide consumers with information online quickly, efficiently, and cheaply. Unlike offline merchants who must rely on a one-time mailing or a small print notice in a catalogue, online merchants (or other site

---

[75] *But see Dwyer* v. *American Express,* 652 N.E.2d 1351 (Ill. App. 1995) (rejecting invasion of privacy claim based on alleged sale of card member lists sorted by buying patterns because customers voluntarily used card and company had ownership interest in data).

[76] *See, e.g., Barnett Bank of West Florida* v. *Hooper,* 498 So.2d 923, 935 (Fla. 1986); *Twiss* v. *State Dept. of Treasury,* 591 A.2d 913, 919–20 (N.J. 1990).

[77] *See, e.g., Pigg* v. *Robertson,* 549 S.W.2d 597, 600 (Mo. Ct. App. 1977).

[78] *See, e.g., Barnsdall Oil Co.* v. *Willis,* 152 F.2d 824, 828 (5th Cir. 1946).

[79] *See, e.g.,* Alaska Sta. § 8.04.662; Ariz. Rev. Stat. § 32–749; Conn. Gen. Stat. § 20–281j.

owners) interact directly with the consumer each time the consumer visits the merchant's site and therefore have the opportunity to educate and interact with the consumer concerning the site's privacy policies before any data collection takes place. Where appropriate, therefore, consumer consent can be requested at the point where a consumer interacts with a site or inquires about a product or service. Moreover, the merchant's ability to control what the consumer sees on any page of its site provides the merchant with a unique ability to educate the consumer about the site's privacy policy. The site can emphasize its participation in a privacy seal program, for example, or provide a link to the site's privacy policy from any page of the site. This in turn can empower consumers to make educated choices about whether they wish to deal with the particular online service based, at least in part, on the level of privacy protection the online operator provides.

The online environment also permits a site to be designed to permit different levels of participation (or provide different types of benefits) based on the consumer's willingness to provide information, or to provide different levels of protection based on consumer demand. Online services also may provide the ability to make data anonymous easily, or to do so selectively upon consumer request. In addition, new technologies, such as P3P and filtering programs, provide consumers with the means to exercise independent control over the level of privacy they obtain while online. Finally, consumers have the ability to vary the level of privacy protection they desire each time they visit an online service or site: The process for providing or withdrawing consent is accessible and can be executed immediately and repeatedly to personalize the level of privacy protection.

Thus, if the online industry takes seriously its obligation to educate and inform consumers, the medium presents enormous opportunities for consumer choice and self-determination. Accordingly, a central pillar of OPA's self-regulatory program is the requirement that an online site notify consumers about the site's data collection and dissemination policies. OPA members are committed to providing consumers with the information and tools they need to make informed choices. A second pillar of OPA's program is ensuring that consumers have the opportunity to make choices: consumers must be able to consent or withhold consent to the use of their data by the site they visit. Lack of consent may manifest itself in the consumer's refusal to use the particular service or continued interaction with the site on a limited level. In some cases, consent or opt-out may be more explicit and permit consumers to participate in the site while blocking only certain secondary uses of the consumer's data.

OPA's program is designed to address the challenges and opportunities provided by the online medium while addressing the U.S. government's and the Directive's data privacy concerns. OPA has adapted these privacy principles to address the Internet industry's enormous, ongoing data flows. In order to enforce the OPA's privacy program and policies, the OPA encourages participation in a seal program that will ensure and enforce a minimum standard level of privacy protection. The seal program must also be easy for consumers to recognize and understand. Seal programs provide the added benefit of being backed up by the FTC's umbrella enforcement authority, state and local consumer protection agencies, and applicable sectoral data privacy regulation.

A. OPA's Privacy Policy Guidelines

In keeping with the key substantive requirements of the Directive and the FTC's privacy principles, the OPA's privacy program addresses notice to data subjects, limitations on use of data, data security and quality, the right to correct personal data, and onward transfers of data. The OPA's program for online data privacy protection is compared with the key requirements of the Directive below.

Notice to Consumers. Because of the rapidly growing ability to collect data about online consumers and the increasing demand for a personalized browsing experience, OPA strongly believes that website operators have a heightened responsibility to make available to online consumers the information necessary to make informed decisions about data privacy. The OPA believes that properly informed consumers should then be allowed to choose the level of privacy that they desire. The OPA therefore requires its members to post a privacy policy that online consumers can view before or at the time that personal data is collected or requested. The privacy policy must, among other things, notify consumers about the online site's data collection practices. The OPA's privacy policy requirement thus is similar to Article 10 of the Directive, which requires data controllers to provide data subjects with information about the controller's identity, the purposes of data processing, and other information necessary to guarantee fair processing. In addition, the privacy policy must be easy to find, read and understand; it also must clearly describe the infor-

mation that is being collected, any possible onward transfers of personal data, and any options that consumers have to refuse to provide data or to block certain uses or transfers of data. OPA further encourages its members to disclose in their privacy policy any consequences of a consumer's refusal to provide information, the accountability or enforcement mechanism(s) used by the organization, and information about how to contact the organization with privacy concerns. By requiring members to provide comprehensive online privacy policies that are easy to find and read, OPA ensures that all online consumers have the information necessary to make an informed decision about whether or not to provide personal information to particular websites, how much information to provide, or whether to even visit certain sites.

Limitations on purposes and onward transfers. Consistent with the OPA's principles regarding notice and consent, the OPA advocates allowing data subjects to opt out of any uses or processing unrelated to the original purpose for which the data are collected. Like Article 6 of the Directive, which requires that personal data not be further processed in a way incompatible with the original purpose for collecting the data, the OPA privacy guidelines limit the extent to which data can be processed for purposes unrelated to the original disclosed purposes in the absence of proper consent. The OPA guidelines similarly limit transfers to third parties for marketing purposes or for other purposes unrelated to the original purposes for collecting the data, much like Articles 10 and 11 of the Directive, which require notifying data subjects of onward transfers of data to third parties where notification is necessary to ensure fair processing of the data. With respect to disclosure of data for marketing purposes, OPA requires its members to disclose in their privacy policies possible onward transfers of personal data and any marketing uses of data. These requirements, and the consumer's ability to leave the site or, in some cases, to opt out of a specific data use on the site, address the principles in Article 14 of the Directive, which provides data subjects with the right to notice prior to disclosure of their personal data for direct marketing purposes and the right to object to direct marketing uses of their data. OPA also encourages its members to take reasonable steps to ensure that third party transferees take reasonable precautions to protect transferred data.

Data quality, access to data, and correction. The OPA supports the Directive's principles of assuring that (1) data are accurate, complete, and timely for their intended purposes, and (2) consumers can access data about them and correct that data where appropriate. However, the extraordinarily wide range of online data processing activities makes it difficult and costly to require all websites to provide consumers with unrestricted access to personal data without regard for its intended purposes or alternative means of ensuring that individuals are informed of data collection and that data quality is maintained as appropriate to those purposes.

Consistent with the spirit of Article 12 of the Directive, which guarantees data subjects the right to access personal data and have that data corrected where necessary, the OPA requires its members to provide "easy mechanisms" for consumers to make inquiries and lodge complaints or objections. The precise mechanisms for such inquiries and the nature and scope of information provided to the consumer on request will necessarily vary according to the data at issue and the costs and benefits associated with furnishing access to the raw data or a summary of the data, given the context of the specific intended uses of the data. For example, some data collected online may be used for electronic commerce transactions or decisions to provide or terminate a service. OPA anticipates that its members would routinely provide access to transaction records and an opportunity to lodge corrections, as these have a substantive impact on the consumer. By contrast, a website may automatically record navigational or "clickstream" data as an individual moves from page to page on a site, either for statistical purposes (to better design and manage the site) or to automatically personalize the initial pages presented to the visitor based on the visitor's historical use of the site. Such information is processed automatically and changes over time. There is little benefit, and much cost, in accumulating this data in a form that could be reviewed intelligibly by the individual at any moment. Moreover, doing so raises additional privacy risks, since it means that more data is readily retrievable by name, and more identifying data must be collected to ensure that the person requesting access is indeed the data subject. Similarly, the use of website data to determine automatically whether to send an individual a product solicitation involves no substantive decision that affects significant consumer interests and does not warrant the cost (and sometimes the increased privacy risks) of storing and providing subsequent access to the data that prompted the solicitation.

Because the online medium entails the possibility of tracking and recording enormous amounts of data on the use of a website, the costs of furnishing unlimited consumer access to all such data would often be prohibitive. The data may not be main-

tained in a manner conducive to consumer-specific access: marketing data, for example, is often coded and stored by categories of merchants or purchases rather than by consumer. Before imposing on website operators (and ultimately on consumers) the costs of providing access to all data resulting from a site visit, the nature and uses of that data must be taken into account. Where data is not used for a purpose that in any way affects the consumer's "fundamental rights or freedoms," or that does not even involve denial of a more mundane benefit to the consumer, the cost and difficulty of access must be given particular weight.

Access by the individual to all data generated online is not the only means of ensuring that consumers (and the relevant enforcement bodies) are aware of the operator's data collection practices and can assess their potential impact. This can often be accomplished, for example, by appropriate notices, consumer education, and monitoring techniques such as the use of "decoys" (pseudonymous registrations to check the manner in which an online service or website uses personal data), rather than by individualized access to vast amounts of non-sensitive data. It is in the nature of online services and websites that it is easy to display notices at the point where information is collected and to give visitors an opportunity at any stage to seek clarification, opt out, or simply leave a site if they are not satisfied with its privacy practices. This offers an efficient means of protecting privacy and should suffice where the data collection is not used for substantive decisionmaking.

Security. Like Article 17 of the Directive, the OPA advocates taking appropriate measures to protect personal data from destruction, loss, misuse or alteration.

Collection of data from children. Well before the passage of the Children's Online Privacy Protection Act, discussed above, the OPA thought it necessary to provide special protection for young Internet users. Out of this concern, the OPA was among the first organizations to adopt principles specifically addressing collection of data from children under the age of 13. These specific principles require OPA members to obtain prior parental consent before collecting any individually identifiable offline contact information from children under the age of 13. Members may collect online contact information from children without obtaining prior parental consent only if they notify parents and allow them to prevent use of the data. Other special protections provided by these OPA principles include requiring members to prevent children from being able to publicly post individually identifiable contact information without prior parental consent; prohibiting members from using special games, prizes or activities to entice children to reveal more information than necessary to participate in the activity; and prohibiting members from distributing to third parties any individually identifiable information collected from a child without obtaining prior parental consent.

B. Enforcement Mechanisms

Although membership in the OPA, standing alone, itself denotes a commitment to privacy protection that arguably could be enforced by the FTC, OPA also advocates that its members commit to an independent enforcement mechanism intended to back up that commitment. OPA promotes participation in a "seal program" by its members as a means of enforcing the OPA privacy guidelines and the member's privacy policies. Seal programs provide participants the right to use an identifiable symbol or logo ("seal") to alert consumers that the participant's online service complies with the seal program's standards; that the participant has procedures to ensure compliance; and that the participant participates in a program designed to resolve consumer complaints.

Seal programs are ideal enforcement mechanisms in the online environment for two reasons. First, seal programs take advantage of the visual nature of websites to alert consumers' attention to privacy policies and practices through the use of visible and easily recognizable graphic seals that can, if desired, be displayed on every page of a site. Second, to some extent seal programs standardize the terms and terminology of privacy practices, making them easier for consumers to comprehend. They give consumers a relatively simple, user-friendly means of identifying websites that have made privacy commitments, linked to greater detail about the site's particular practices.

In many seal programs, participants cede a degree of investigative or complaint resolution authority to the seal program's enforcement entity. The entity often is permitted to disclose complaints to the public and government agencies, and the entity can drop a company that fails to conform with the required conduct. Moreover, seal programs may provide government agencies with a hook to mix self-enforcement with government regulation: as discussed in Part I above, a company's public affirmation of participation in a seal program would provide the FTC (or other con-

sumer protection entity on the state or local level) with the grounds to prosecute a company's failure to in fact uphold the standards articulated by the seal program.

A seal program meeting OPA's criteria would enhance data privacy protection by requiring that seal participants live up to the types of privacy guidelines advocated by OPA, as well as any additional policies the seal program adopts. OPA does not, at least currently, intend to operate its own seal program, and it has not endorsed a specific program to date. In reviewing seal programs, however, OPA would expect a commitment to at least the same degree of privacy protection espoused by the OPA, as well as the following enforcement practices and policies:

Participation from outside the business community. OPA suggests that the seal program obtain input from representatives of consumer advocate groups and academia, in addition to representatives of the business community.

Verification and monitoring. Prior to awarding the seal to an organization, the seal program must require participants to submit to a compliance review by the seal program or provide a self-assessment verifying that the organization is in compliance with the program's standards. Once the seal has been awarded, participants must consent to periodic verification in the form of auditing, periodic reviews, or use of pseudonymous "decoys" or other technological monitoring.

Complaint resolution. The seal program must require participants to provide an easy-to-use consumer complaint resolution process that will serve as the consumer's first remedy. If the participant and consumer are unable to resolve a complaint through the participant's internal dispute resolution process, the participant must then submit to the seal program's complaint resolution mechanism. In addition to these mechanisms, consumers must not be prohibited from pursuing any other legal remedies that may be available to them under federal or state law.

Penalties or noncompliance. Failure to comply with the requirements of the seal program (and in particular, failure to follow the program's dispute resolution requirements) should result in placing the participant on probation or instituting proceedings to revoke the participant's right to use the seal.

Monitoring for misuse or misappropriation. The seal program should monitor use of the seal and if necessary, bring litigation to prevent unauthorized use of the seal. In addition, the seal program must refer non-complying companies to appropriate government agencies, including the FTC.

Education and outreach. The seal program must educate consumers and businesses about the seal program and online privacy issues. These education and outreach efforts should include providing publicity for participants, publicly disclosing seal revocation and material non-compliance, and periodically publishing verification and monitoring procedures.

To date, two major seal program initiatives are underway or about to be launched that may embody the policies and practices advocated by the OPA: TRUSTe and BBB*OnLine*. The OPA is monitoring the development of those programs and others to determine whether they meet OPA's requirements for privacy protection and effective enforcement.

The TRUSTe program, which began as a collaboration between the Electronic Frontier Foundation and CommerceNet, has been administering its online privacy seal program since June of 1997. This program requires participants to post an online privacy policy that meets TRUSTe guidelines, to submit to TRUSTe oversight, and to cooperate with TRUSTe's dispute resolution efforts. In return, participants are given the right to display TRUSTe's seal on their home page. This seal serves as a link to the company's privacy policy, and consumers can also verify the authenticity of the seal online.

The privacy policy required of TRUSTe participants must explain what data are being collected, the purposes of data collection and processing, with whom the data will be shared, the consumer's options concerning processing and onward transfers, data security procedures that are in place, and how consumers can update or correct data. Licensees who join or renew after October 1998 must also give consumers the opportunity to opt out of secondary or third-party uses of data provided by the consumer. Also in October 1998, TRUSTe introduced a Children's Privacy Seal Program that applies to websites directed specifically at children under the age of 13, as well as sites that collect age-specific information. The children's program requires site operators to notify parents and obtain their consent before collecting and using a child's online or offline contact information. Sites aimed specifically at children must post the unique "kid's seal."

TRUSTe utilizes a variety of verification and enforcement techniques. In cases where TRUSTe suspects that a participant is not complying with program guidelines or with the participant's own privacy policy, the participant may be subject to on-site compliance reviews by TRUSTe's official auditors, revocation of the right to

use the TRUSTe seal, termination from the TRUSTe program, and referral to appropriate government agencies.

The Better Business Bureau ("BBB") runs the largest and most recognized retail, service and national advertising self-regulation and consumer dispute resolution programs in the United States. Using its self-regulatory models as a starting point, the BBB has been operating an online seal program (with more than 2000 participants) through BBB*OnLine* since mid-1997. BBB*OnLine* assists consumers in finding reliable online merchants that have agreed to BBB standards for truthful advertising and customer satisfaction. BBB*OnLine* has proposed a privacy program that likely will be similar in many ways to the TRUSTe program and will utilize BBB*OnLine's* existing self-regulatory framework.

BBB*OnLine* is still in the process of developing its privacy principles. These principles are expected to be similar to those of the OPA and TRUSTe programs, although they may in some respects provide additional privacy protections not currently required by the OPA and TRUSTe. The BBB*OnLine* enforcement framework will consist of use of a recognizable seal to assert compliance with BBB*OnLine* principles and the company's privacy policy, a comprehensive annual compliance assessment, additional independent verification measures, consumer dispute resolution, and appropriate referrals by BBB*OnLine* to the FTC and other government authorities. BBB*OnLine* participants will have to respond promptly to all consumer complaints, submit to BBB*OnLine's* dispute resolution process, and maintain a satisfactory complaint handling record with the BBB. BBB*OnLine* will refer eligible complaints to a free, informal dispute resolution process patterned after BBB's national advertising review program, and BBB will make that process available for complaints about non-seal participants as well as seal participants. BBB*OnLine* also will refer uncooperative or non-compliant companies to the FTC or other appropriate federal or state regulatory agencies.

IV. CONCLUSION

As Articles 25(2) and 27 of the Directive make clear, the EU has recognized that industry and professional standards can be powerful tools for protecting data privacy. In the United States, industry-wide self-regulation of data privacy can be an especially effective means of ensuring that consumer data receives the level of protection embodied in the EU Directive where such self-regulation combines private sector standards with FTC enforcement, regulation by federal and state agencies and, where appropriate, enforcement by the courts.

In the online environment, OPA has established principles—principles its members must publicly embrace—that are consistent with the policies of the U.S. government and with the Directive. OPA members must submit to dispute-resolution procedures, and, by publicly embracing OPA's principles, members are also subject to potential enforcement by the FTC and other government agencies. The emergence of two online privacy seal programs demonstrates that the enforcement element of OPA's self- regulatory framework is not just hypothetical, but is quickly developing. Moreover, these seal programs are not engaging in a "race to the bottom," but rather, in keeping with the recent initiatives and pronouncements of the U.S. government, they are embracing meaningful principles embodying a significant degree of privacy protection. In addition, OPA members frequently will be subject to additional regulation of various types of data protection on both the state and federal level, enforced by government agencies and the courts. Self-regulatory programs such as OPA's, which are designed to operate in the context of the United States' layered approach of self-regulation backed by government enforcement, should be recognized as effective by the EU in its effort to protect privacy while promoting the uninterrupted flow of global commerce.

W. SCOTT BLACKMER
(sblackmer@wilmer.com),
LYNN CHARYTAN
(lcharytan@wilmer.com),
WILMER, CUTLER & PICKERING,
Washington, DC.

The CHAIRMAN. Mr. Berman.

STATEMENT OF JERRY BERMAN

Mr. BERMAN. Thank you, Senator. Mr. Chairman, Senator Leahy, Senator Kohl, Senator Schumer, I appreciate the opportunity to be here to talk about privacy on the Internet.

While I agree with the caution and concerns of the previous witnesses, I want to endorse them, but also try and reposition the issue somewhat. I think we have to step back and say what are we doing here. The Internet is not just a commercial forum; it is the future community for many of us and for many of our transactions going into the 21st century. There are 160 million people on the Internet. It is eventually going to be all of us because we are moving our transactions. We are going to do business there; our libraries are there, medical records are there. We are putting entertainment there. We are building new communities.

In all due respect, and it is true, without all the hype, we are building a "virtual me" and virtual communities, and that means that we are now looking at developing the fundamental rules for this Internet. It is almost like constitution-building, in my view. It is a global Internet, and that makes it difficult. We are not just all sitting in Philadelphia writing the rules for the world, but we are trying to figure out what the fundamental law is.

My organization wants to ensure that there is a commerce clause, but that there is also a bill of rights, and that means that we have to look at the Internet from several perspectives. First, the key thing to understand about the Internet is that it is a different architecture. It is global, decentralized, interactive, which changes the characteristics.

It is very important for Congress to understand its architecture. Not understanding the architecture in the Communications Decency Act—it is 0 for 2 in terms of writing legislation, so a careful look at how the Internet works and why it is different than other media is very important.

Second, the goal has to be privacy. It is not legislation or self-regulation; it is privacy. And what do we mean by privacy? Privacy is not just protection against commercial users of information misusing my information. The government is also on the Internet. Law enforcement is also on the Internet. We just published a study of government Web sites. Two-thirds of all government sites haven't got a privacy policy up. They are doing business on the Internet.

Senator Leahy's E-RIGHTS bill deals with how do we balance law enforcement needs and privacy in this new community. How is law enforcement going to be done? How are they going to relate to these new databases that are at AOL or on the Net, the digitalme that Novell talks about? So it is both privacy expectations against the government and the private sector. And self-regulation may work a great deal in the private sector up to a point, but I don't know how you solve the government problem without drawing law to limit and define the rights of citizens as against the government.

When we talk about privacy, we have to break it down into several expectations. The first expectation that we have when we go on the Internet or into any community is that we have a certain amount of autonomy, what Senator Leahy talked about in Ver-

mont, the right to be let alone, not to be identified, to shop, to browse. The Internet can afford that, but also the technologies like the Intel chip, which is an identity chip which may identify each one of us as we go through the Internet, cookies. You have heard of the technologies that are tracking and collecting information about citizens, not for bad purposes, but to make the Net more efficient, to sell commerce, to get people to the sites that they want to go to. But there is a rich, new source of information on the Internet, and the question is will citizens have the autonomy to be left alone.

Second, the key to that is at least fair information practices. We go on the Net and we want to know when information is collected about us, where it is going, how is it going to be used, and do we have choices about that. That is fair information practices and it is the key. It helps us to know whether we have any autonomy. We have to ensure that those fair information practices are on the Net.

The bad news is that we are very far behind. Only 14 percent of all Web sites post what their privacy policies or information policies are. The good news is that the business community and everyone understands that it is good for business and commerce, and that consumers will not trust the Internet until those policies are there.

Third, consumers want confidentiality. They want confidentiality in their communications. This committee, in 1986—Senator Hatch, Senator Leahy—wrote the Electronic Communications Privacy Act which created new privacy rights for e-mail. The whole issue of encryption—because of the decentralized nature, that debate over encryption and technology policy is critical. There are new databases that are being created on the Internet, like digitalme, which are as sensitive as our wallet that is still there, but we are now shopping with on the Net. What are the protections against government for that?

So we have to come back and say, well, what are the solutions? There are a bundle of solutions. Partly, it is technology, the Platform for Policy Preferences which allows people to express privacy policies on the Net. Partly, it is self-regulation, like BBBOnLine and TRUSTe, which is telling consumers and getting sites to disclose what their policies are. That will work up to a point.

And I think that IBM and AOL and the Privacy Alliance are in the lead of establishing what the baseline rules are for fair information practices on the Net, but it will only go up to a point. At some point, you are going to have to deal with the bad actor on the Net, define what is a violation of privacy on the Net. In other words, you can't just say, well, this is what I am going to promise you about your information, but if I don't do it, what are the remedies? There may be some private sector remedies, but what is the role of the FTC there?

You have to go very carefully here because you are dealing with information, and information raises First Amendment issues. The remedies have to be clear, concise and not vague, so that a lot of thinking has to go into what is the remedy for someone misusing your address and personal information in a commercial transaction versus a medical transaction. One size does not fit all. And then we are going to need legislation.

To conclude, it is a series of things that we have to look at. We are at the beginning of trying to define the constitution for cyberspace. I think that there are several ways that you can go. One, Senator Hatch and Senator Leahy participated a decade ago in bringing the private sector and the privacy community and industry and policymakers together to define the Electronic Communications Privacy Act. That was a dialogue reaching consensus. No privacy legislation has ever been done without consensus between the private sector and the privacy community. It just never happened. So, that consensus is important. Senator Kohl's idea of a commission 25 years after the last commission, with the whole Internet, is a good idea for trying to sort out some of these problems.

So I think we are at the beginning. We are anxious to work with all of you to try and define these issues. We think that this is a critical part of the new society that we are moving into, and I appreciate the opportunity to testify here today. Thank you.

The CHAIRMAN. Thank you, Mr. Berman.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF JERRY BERMAN

I. OVERVIEW

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify on the issue of individual privacy in the online environment. CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

CDT focuses much of its work on the Internet because we believe that it more than any other media has characteristics—architectural, economic, and social—that are uniquely supportive of First Amendment values. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu.

But while the First Amendment potential of the Internet is clear, and recognized by the Court, the impact of the Internet on individual privacy is less certain. Will the online environment erode individual privacy-building in national identifiers, tracking devices, and limits on autonomy? Or will it breathe new life into privacy—providing protections for individuals' long held expectations of privacy?

As we move swiftly toward a world of electronic democracy, electronic commerce and indeed electronic living, the need to construct a framework of privacy protection that fits with the unique opportunities and risks posed by the Internet is critical. But as Congress has discovered in its attempts to regulate speech, this medium deserves its own analysis. Laws developed to protect interests in other media should not be blindly imported. To create rules that map onto the Internet we must fully understand the characteristics of the Internet and their implications for privacy protection. We must also have a shared understanding of what we mean by privacy. Finally we must assess how to best use the various tools we have for implementing policy—law, computer code, industry practices, and public education—to achieve the protections we seek.

II. WHAT MAKES THE INTERNET DIFFERENT?

As Congress considers crafting rules to protect privacy on the Internet, it must first understand the specific challenges to privacy posed by the Internets' functions and use.

A. Increased data creation and collection

The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital finger-

prints reveal a great deal about an individual's life. This increasingly detailed information is bought and sold as a commodity by a growing assortment of players and often sought by government.

B. The globalization of information and communications

On the Internet, information and communications flow unimpeded across national borders. The Internet places the corner store, and a store three continents away, equally at the individual's fingertips. Just as the flow of personal information across national borders poses a risk to individual privacy, citizens' ability to transact with entities in other countries places individual privacy at risk in countries that lack privacy protections. Whether protecting citizens from fraud, limiting the availability of inappropriate content, or protecting privacy, governments are finding their traditional ability to make and effectively enforce policies challenged by the global communications medium.

C. Lack of centralized control mechanisms

The Internet's distributed architecture presents challenges for the implementation of policies. The Internet was designed without gatekeepers—there is no single entity that controls the flow of information. And as individuals and governments continually discover, the Internet offers users an unequalled ability to route around unwanted attempts to control activities and communications.

III. WHAT DO WE MEAN BY PRIVACY, AND HOW IS IT BEING ERODED?

There are several core "privacy expectations" that individuals have long held vis-a-vis both the government and the private sector, the protection of which should carry over to interactions on the Internet.

A. The expectation of autonomy

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. Individuals believe that if they have not affirmatively disclosed information about themselves, then no one knows who they are or what they are doing. But, counter to this belief, the Internet generates an elaborate trail of data detailing every stop a person makes on the Web. The individual's employer may capture this data trail if she logged on at work, and it is captured by the Web sites the individual visits. Transactional data, click stream data, or "mouse-droppings" can provide a "profile" of an individual's online life.

Two recent examples highlight the manner in which individuals' expectation of autonomy is challenged. (1) The introduction of the Pentium III processor equipped with a unique identifier (Processor Serial Number) threatens to greatly expand the ability of Web sites to surreptitiously track and monitor online behavior. The PSN could become something akin to the Social Security Number of the online world—a number tied inextricably to the individual and used to validate one's identity throughout a range of interactions with the government and the private sector. (2) The Child Online Protection Act (COPA), passed in October, requires Web sites to prohibit minors' access to material considered "harmful to minors." Today when an individual walks into a convenience store to purchase an adult magazine they may flash their id. Under the COPA an individual will instead be asked to not only flash their id, but also to leave a record of it and their purchase with the online store. Reliance on such systems will create records of individuals' First Amendment activities, thereby conditioning adult access to constitutionally protected speech on a disclosure of identity. The defenses pose a Faustian choice to individuals seeking access to information—protect privacy and lose access or exercise First Amendment freedoms and forego privacy.

B. The expectation of fairness and control over personal information

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Whether it is medical information, or a record of a book purchased at the bookstore, or information left behind during a Web site visit information is routinely collected without

the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

The Federal Trade Commission report from last June, "Privacy Online: A Report to Congress," found that despite increased pressure businesses operating online continue to collect personal information on the World Wide Web without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that while 92 percent of the sites surveyed were collecting personally identifiable information only 14 percent had some kind of disclosure of what they were doing with personal data.

In a CDT study of federal agency Web sites, last week, we found that just over one-third of federal agencies had a "privacy notice" link from the agency's home page. Eight other sites had privacy policies that could be found after following a link or two and on 22 of the sites surveyed we could not find a privacy policy at all.

C. The expectation of confidentiality

When individuals send e-mail they expect that only the intended recipient will read it. In passing the Electronic Communications Privacy Act in 1986, Congress reaffirmed this expectation. Unfortunately, it is once again in danger.

While United States law provides e-mail the same legal protection as a first class letter, the technology leaves unencrypted e-mail as vulnerable as a postcard. Compared to a letter, an e-mail message is handled by many independent entities and travels in a relatively unpredictable and unregulated environment. To further complicate matters, the e-mail message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the privacy protections are likely to stop at the border.

E-mail is just one example. Today our diaries, medical records, and confidential documents are more likely to be out in the network than stored in our homes. As our wallets become "e-wallets" housed somewhere out on the Internet rather than in our back-pockets, the confidentiality of our personal information is at risk.

The advent of online datebooks, and products such as Novell's "Digital Me", which invite individuals to take advantage of the convenience of the Internet to manage their lives, raise increasingly complex privacy questions. While the real "me" has Fourth and Fifth Amendment protections from the government, the "Digital Me" is increasingly naked in cyberspace.

IV. WHERE DO WE GO FROM HERE?

It is clear that our policy framework did not envision the Internet as we know it today, nor did it foresee the pervasive role information technology would play in our daily lives. Our legal framework for protecting individual privacy in electronic communications, while built upon constitutional principles buttressed by statutory protections, reflects the technical and social "givens" of specific moments in history. Crafting privacy protections in the electronic realm has always been a complex endeavor. Reestablishing protections for individuals' privacy in this new environment requires us to focus on both the technical aspects of the Internet and on the practices and policies of those who operate in the online environment.

A. The importance of architecture

Understanding the context is central to all effective efforts to protect privacy. While the global, distributed network environment of the Internet raises challenges to our traditional methods of implementing policies, the specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example a privacy-protective architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy and ensuring the expectations of privacy. A privacy-protective architecture would enable individuals to control when, how, and to whom personal information is revealed. It would also provide individuals with the ability to exercise control over how information once disclosed is, if at all, subsequently used. Finally, a privacy-protective Internet architecture would provide indi-

viduals with assurance that communications and data will be technically protected from prying eyes.

While there is much work to be done in the designing of a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in efforts like the Anonymizer, Crowds, and Onion Routing that shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit. The World Wide Web Consortium's Platform for Privacy Preferences ("P3P") is also a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to drive openness about information practices to encourage Web sites to post privacy policies and to provide individuals with a simple automated method to make informed decisions. Through settings on their Web browsers, or through other software programs, users will be able to exercise greater control over the use of their personal information.

Technologies must be a central part of our privacy protection framework, for they can provide protection across the global and decentralized Internet where law or self-regulation alone may prove insufficient.

B. Protecting the privacy of communications and information

Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. The Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored on servers controlled by third parties. Daily interactions such as our choice of articles at a news Web site, our search and purchase of an airline ticket, and our use of an online date book to manage our schedule such as Yahoo's calendar leave detailed information in the hands of third-parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: (1) the traditional Fourth Amendment standard for records stored on an individual's hard drive or floppy disks; (2) the Title III-Electronic Communications Privacy Act standard for records in transmission; (3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record; and (4) a statutory standard allowing subpoena access and delayed notice for records stored on a remote server such as the diary of a student stored on a university server, or personal correspondence.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

While Congress took the first small step towards recognizing the changing nature of transactional data with amendments to the Electronic Communications Privacy Act enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), the increase in transactional data and the increasing detail it reveals about individuals' lives suggests that these changes are insufficient to protect privacy.

Moreover, the Electronic Communications Privacy Act must be updated to provide a consistent level of protection to communications and information regardless of where they are stored and how long they have been kept. Technologies that invite us to live online will quickly create a pool of personal data with the capacity to reveal an individual's travels, thoughts, purchases, associations, and communications. We must raise the legal protections afforded to this growing detailed data regardless of where it resides on the network.

C. Establish rules that give individuals control over personal information during commercial interactions

We must adopt enforceable standards, both self-regulatory and regulatory, to ensure that information provided for one purpose is not used or redisclosed for other purposes without the individual's consent. All such efforts should focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare in 1973. The challenge of implementing privacy practices on the Internet is ensuring that they build upon the medium's real-time and interactive nature

to foster privacy and that they do not unintentionally impede other beneficial aspects of the medium.

Historically, for privacy legislation to be successful, it must garner the support of at least a section of the industry. To do so, it must build upon the work of some industry members—typically binding bad actors to the rules being followed by industry leaders—or be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act.

Today, the dialogue over assuring privacy on the Internet and in electronic commerce is well situated for a successful legislative effort. Consensus exists around at least four general principles: notice of data practices; individual control over the secondary use of data; access to personal information; and, security for data. However, the specifics of their implementation and the remedies for their violation are just beginning to be explored by all interested parties. When is information identifiable? How is it accessed? How do we create meaningful and proportionate remedies that address the disclosure of sensitive medical information as well as the disclosure of inaccurate marketing data? These hard issues must be more fully resolved before the policy process will successfully move forward. The leadership of Internet-savvy members of this Committee and others will be critical if we are to provide workable privacy protections for the Internet.

D. A privacy protection entity to provide expertise and institutional memory, a forum for privacy research, and a source of policy recommendations on privacy issues

The work outlined above, and the state of privacy today, all weighs in favor of creating a privacy entity within the federal government. The existing approach has hindered the development of sound policy and failed to keep pace with changes in technology. While we are pleased with the Administration's recent appointment of Peter Swire to the Office of Information and Regulatory Affairs as the federal "privacy czar," we believe that OIRA is incapable, due to institutional constraints and a lack of autonomy, of addressing several key privacy issues. The United States needs an independent voice empowered with the scope, expertise, and authority to guide public policy. Such an entity has important roles to play on both domestic and international fronts. It would serve as the forum for collaboration with other governments, the public interest community, and the business community.

V. CONCLUSION

No doubt, privacy on the Internet is in a fragile state. However, there is new hope for its resuscitation. There is a special need now for dialogue. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. Cooperation among the business community and the nonprofit community is crucial. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or developing legislation—none will happen without a forum for discussion, debate, and deliberation. We thank the Committee for providing this initial forum and look forward to working with the members and staff and other interested parties to foster privacy protections for the Digital Age.

The CHAIRMAN. Mr. Bodoff.

STATEMENT OF RUSSELL T. BODOFF

Mr. BODOFF. Thank you. Mr. Chairman and members of the committee, I am pleased to present to you our BBBOnLine Privacy Seal program and to share the experience of our first month of operation, after our official launch of the program which took place on March 17.

BBBOnLine is a subsidiary of the Council of Better Business Bureaus, with the start-up of our BBBOnLine privacy initiative supported by 24 leading-edge sponsoring companies. The program benefits from the Better Business Bureau's 100-percent name recognition, as well as the BBB's 86 years' experience in voluntary self-regulation and consumer dispute resolution.

Our privacy program awards an easily recognizable seal to businesses that post online privacy policies meeting rigorous principles, including notice to consumers, disclosure, choice and consent, ac-

cess, and security. It offers a separate and distinct seal for sites directed at children. It provides a thorough and consumer-friendly dispute resolution system. It monitors compliance through a comprehensive assessment of a company's online privacy practices, and it takes specific actions for non-compliance, such as seal withdrawal, publicity and referral to government enforcement agencies.

To qualify for a privacy seal, companies must submit an application and successfully complete a comprehensive assessment process that investigates over 170 different aspects of an applicant's information practices. The founding principle of our privacy program is that it requires privacy seal participants to say what they do, to do what they say, and have it verified.

This begins with an easy to find and easy to understand privacy notice. Privacy notices must be one click away from a Web site's home page and from every other page where personally identifiable information is collected. Depending on the information practices of the participant, this privacy notice may contain as many as 16 required disclosures, but it will always describe who is collecting the information, what type of information is being collected, and how that information is used and shared. It will always disclose how an individual can access and correct their information, how to contact the company, and how to contact BBBOnLine.

While evaluating the privacy notice is critically important, the BBBOnLine assessment does not stop there, but looks further into the actual information practices of a company. Participants must have in place reasonable security measures to prevent unauthorized access to both stored and transmitted data. This includes doors and locks, adequate training for employees, adequate logs and recordkeeping, and a mandatory use of encryption when there is a receipt or transmission of sensitive information, such as credit card numbers, health care data or Social Security numbers.

Seal participants must provide a means by which individuals can gain reasonable access to all the maintained and retrievable personally identifiable information they submit online. Seal participants that operate Web sites or online services that are directed to children under the age of 13 must also complete an additional children's assessment process.

BBBOnLine's privacy program's free, convenient and speedy dispute resolution service offers the assistance of trained professionals to ensure that consumers have a simple and effective way to have their concerns addressed. Consumers can contact the BBBOnLine dispute resolution intake center via e-mail, toll-free telephone call, or by following the instructions on our Web sites.

As remedies, consumers can seek to have the information which was submitted online used only in a manner consistent with the company's published privacy policy and/or the consumer can seek to have inaccurate information corrected. BBBOnLine may also require corrective action in the form of a change in the seal participant's online privacy policies or practices if, based on evidence in the case, it finds such action to be required to avoid return to the same complaint.

The program will also monitor compliance through a system of random audits to ensure that program participants remain in compliance. We have designed our program to have serious and effec-

tive consequences for non-compliance. In our dispute resolution process, we will publish decisions so the public will be able to monitor resolution of complaints about violations of privacy policies.

The Privacy Seal program has been officially open now for about 1 month. Since the launch, we have already processed over 240 formal applications. We have awarded 14 seals and have many other companies ready and close to approval. The response has been impressive and more applications are coming in everyday. Companies are reporting to us that the assessment process is so thorough that it requires them to carefully evaluate and in some cases change their entire data-collecting and processing practices.

Now that we are open for business, we are engaging in an aggressive outreach program to educate businesses on good privacy practices. For example, we recently entered into an agreement with the American Electronics Association to educate their 3,000 members about good privacy principles. Similar business outreach will be announced shortly with other major trade associations, as well as our Better Business Bureaus. Next on our agenda will be developing a major outreach to consumers and children to help them better understand how to protect their privacy while they are online.

In closing, let me say how excited we are that the BBBOnLine privacy program, which was created in less than 9 months, is already being described as the most comprehensive privacy self-regulation anywhere in the world. Consumers have a high level of trust in our organization. A study released last week by AT&T Research Labs indicated that a privacy notice on a Web site, along with the Better Business Bureau seal, gave a consumer a higher level of confidence than even privacy regulation.

I want to thank the committee members for their attention, and I hope that you share our enthusiasm about the tremendous progress that has been made.

The CHAIRMAN. Thank you, Mr. Bodoff.

[The prepared statement of Mr. Bodoff follows:]

PREPARED STATEMENT OF RUSSELL T. BODOFF

Mr. Chairman and members of the Committee, my name is Russell Bodoff, I am Senior Vice President and Chief Operating Officer of BBB*OnLine,* an independent subsidiary of the Council of Better Business Bureaus. I am pleased to present to you the BBB*OnLine* Privacy Seal program and to share the experience of our first month of operation after the official launch of the program on March 17, 1999.

The Council of Better Business Bureaus (CBBB) is the umbrella organization for the nation's Better Business Bureau system, which consists of over 130 local BBB's and branches and 270,000 member businesses across the United States. The CBBB is a nonprofit business membership organization tax exempt under section 501(c)(6) of the Internal Revenue Code. More than 325 leading edge companies nationwide belong to the CBBB and provide support for its mission of promoting ethical business practices through voluntary self-regulation and consumer and business education.

Each year, millions of consumers contact the Better Business Bureau for pre-purchase information or for assistance in resolving marketplace disputes. In large part, they are drawn to the BBB by its enormous name recognition. The BBB trademark is one of the country's most widely recognized by both business and consumers (100 percent business and 98 percent consumer brand recognition according to a 1996 Gallup Poll). The public looks to the Better Business Bureau for impartial and reliable information on a broad range of companies, products and services. We. provide reliability reports on individual businesses (members and non-members), issue reports on publicly soliciting charitable organizations and provide consumer advisories on a host of offers, promotions and scams. We offer consumers and businesses a

means to resolve disputes through conciliation, mediation and, when necessary, arbitration. In fact, the BBB operates one of the, if not the, largest out-of-court consumer/business dispute settlement program in North America.

Through its partnership with the major advertising trade associations, the American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA), and the American Advertising Federation (AAF), the CBBB also operates a highly successful and much praised advertising self-regulation program that helps assure truthful advertising and appropriate advertising directed to children.

Our name recognition, the extremely high level of trust we have earned from the public, and our experience in operating self-regulation and dispute settlement programs, including our previous experience with offering another seal program in the BBB*OnLine* Reliability Program, are some of the reasons the business community and the Administration asked BBB*OnLine* once again to provide a framework for self-regulation in the major issue of concern in online commerce—personal privacy protection.

BBB*OnLine* is a 501(c)(6) tax exempt organization, supported by leading online marketing and technology companies in the United States. A wholly owned subsidiary of the CBBB, BBB*OnLine* was established by the CBBB and its member sponsors as a means to promote the highest ethical business practices online through self-regulation and consumer education and self-help measures, and thereby help to foster consumer trust and confidence in this new market. The online marketplace has vast potential for consumers and business alike. However, it presents risks to consumers who can not easily determine the reliability of any given company by simply looking at its website, and it makes it difficult for an ethical business to distinguish itself from a fly-by-night operator.

To help online companies distinguish themselves, BBB*OnLine* provides two separate seal programs for online businesses—the Reliability Seal Program and the Privacy Seal Program—and provides consumer information through our website, www.bbbonline.org.

The BBB*OnLine* Reliability Program was launched in April of 1997 with the support of 11 major corporate sponsors. The objective was to provide a resource for consumers seeking trustworthy businesses on the Internet; to help legitimate businesses distinguish themselves from fly-by-night operators; and to demonstrate that self-regulation of the online marketplace can succeed. To participate in the Reliability Program a company must be a BBB member, cooperate with CBBB's National Advertising Division (NAD), Children's Advertising Review Unit (CARU) and National Advertising Review Board (NARB) and commit to third-party dispute resolution. Over 2,900 companies from various sectors and of various sizes have been approved to date for the Reliability Seal and we are currently approving 200 new participants each month. Some of the largest marketing sites on the Internet participate in the program. Posting the Reliability Seal on a website provides consumers with an easy means to check a company's history, obtain contact information, and be assured that the company stands behind its advertising claims. A BBB representative visits, in person, the physical office of each and every Reliability Seal applicant, to ensure that they are who and where, they say they are.

Launched in March 1999, the BBB*OnLine* Privacy Program is the only privacy seal program that is rooted in 86 years of experience in voluntary self-regulation and consumer dispute resolution. The BBB*OnLine* Privacy Program awards seals to online businesses verified as meeting our high standards including: the posting of online privacy policies meeting rigorous privacy principles, completion of a comprehensive evaluation, monitoring and review by a trusted organization, and participation in a consumer dispute resolution system. For further detail, please visit www.bbbonline.org/businesses/privacy/eligibility.html.

After the successful creation and implementation of the BBB*OnLine* Reliability Program, it was a natural progression for BBB*OnLine* to address the significant issues pertaining to privacy in electronic commerce. BBB*OnLine* agreed to design a new BBB*OnLine* privacy self-regulation program in June of 1998. There was tremendous industry support for this effort. Twenty-four major companies provided start up funds of $2.3 million to develop the program design. Currently seventeen companies serve as full corporate sponsors: Ameritech, AT&T, Bank of America, Dun & Bradstreet, Eastman Kodak, GTE, Hewlett-Packard, Microsoft, Netscape, Procter & Gamble, Reed Elsevier (LEXIS-NEXIS), Road Runner Group, Sony Electronics, US WEST, Visa and Xerox. Plus, twenty-four companies support and participate in our privacy steering committee: America Online, American Express, AMR Corporation (American Airlines and Travelocity), AT&T, Bank of America, Dell, Dun & Bradstreet, Eastman Kodak, Equifax, Experian, Ford, Hewlett-Packard, IBM, Intel, J.C. Penney, MCI WorldCom, Microsoft, New York Times Electronic Media, Nickelodeon, Procter & Gamble, Reed Elsevier (LEXIS-NEXIS), Sony Electronics,

US WEST, and Xerox. In addition to the financial support provided by our founding sponsors, a steering committee of supporting companies was formed to assist BBB*OnLine* in developing a self-regulatory program that was substantive, realistic, and workable. Contributing to this effort were privacy experts such as Professor Alan Westin of Columbia University and Dr. Mary Culnan of Georgetown University. We also created a separate dispute resolution committee to help design a dispute resolution component to the program to deal with the specialized area of privacy disputes.

The Privacy Program is designed to be a user-friendly tool that helps foster trust and confidence on the Net. It is also designed to be a valuable resource for business as a simple, one-stop, non-intrusive way to demonstrate compliance with credible online privacy principles.

The core of the BBB*OnLine* Privacy Program:

- Awards an easily recognizable and affordable "seal" to businesses that post online privacy policies meeting rigorous principles, including notice to consumer, disclosure, choice and consent, access, and security;
- Offers a separate and distinct seal for sites directed at children;
- Provides a thorough and consumer-friendly dispute resolution system;
- Monitors compliance through requirements that participating companies undertake, at a minimum annually, assessments of their online privacy practices; and,
- Takes specific actions for non-compliance, such as seal withdrawal, publicity and referral to government enforcement agencies.

Applicants eligible to participate in the BBB*OnLine* Privacy program must post a clear and easy to find privacy notice and operate a website or online service that is directed to U.S. residents. To reach broadly, BBB membership is not required to participate in the privacy program, although applicants can not have an unsatisfactory BBB record.

To ultimately qualify for a privacy seal, applicants must submit an application and successfully complete a comprehensive assessment process that investigates over 170 different aspects of an applicant's information practices, including privacy notice content and placement, corporate structure, security measures, transfer and merger of information, access, correction; and (if the website or online service falls within our children's guidelines) a comprehensive set of additional children's requirements. For more information, please visit www.bbbonline.org/businesses/privacy/assess-html.html or see Appendix A.

The assessment process itself was field tested with a diverse group of companies to make sure that its objective of performing an in-depth evaluation of information practices was user friendly for business and workable in performing an effective analysis of the way a seal applicant collects and uses personal information. The assessment process offers companies an excellent benchmark for evaluation and implementation of sound privacy policies and practices.

After successfully completing the assessment process, applicants must then have a company officer sign a participation agreement that obligates them to submit to random and independent third party verification, to utilize the BBB*OnLine* Dispute Resolution process, and to notify BBB*OnLine* whenever there is a material change in either (1) their privacy notice, (2) their information practices, and/or (3) the scope of the privacy seal.

The essence of the BBB*OnLine* Privacy Program is that it requires privacy seal participants to "Say What You Do, Do What You Say, and Have It Verified."℠ This begins with a clear and easy to find privacy notice. Privacy notices must be "one click away", from a website's homepage *and* every other page where personally identifiable information is collected. Depending on the information practices of the participant, this privacy notice may contain as many as 16 required disclosures, but it will always describe who is collecting information, what types of information is being collected, and how that information is used and shared. It will always disclose how an individual can access and correct their information, how to contact the participant, and how to contact BBB*OnLine.* Mandatory opt-outs are required whenever information will be transferred to third parties for marketing, and whenever information is used in a way not described in the privacy notice.

While evaluating the privacy notice is critically important, the BBB*OnLine* assessment does not stop there, but looks further into the actual information practices of an applicant.

Seal participants must have in place reasonable security measures to prevent unauthorized access to both stored and transmitted data. This includes doors and locks, adequate training for employees, adequate logs and record keeping, and a mandatory use of encryption when there is a receipt or transmission of sensitive in-

formation such as credit card numbers, health care data, and social security numbers.

In addition to disclosing information transfer practices and providing opt-outs if such transfers are for marketing purposes, seal participants must also take steps to ensure that transferred information continues to be used only in the ways disclosed in the privacy notice and according to the choices made by an individual. Seal participants must also follow special rules when information is submitted online by one person about someone else, such as with gift recipients.

Seal participants must provide a means by which individuals can gain reasonable access to all the maintained and retrievable personally identifiable information they submit online, and establish a reasonable process by which seal participants can verify the identity of those requesting access.

Seal participants that operate websites or online services, or portions thereof, that are directed to children under 13, or at which information is collected from visitors actually known to be children under 13, must also complete a children's supplemental assessment questionnaire and assessment process based upon the requirements of the Children's Online Privacy Protection Act of 1998, and the guidance set forth by both the Online Privacy Alliance, and the Council of Better Business Bureaus' Children's Advertising Review Unit.

Such children's websites must acquire prior verifiable parental consent before a child's information can be collected and before children are given the ability to post identifying information. Reasonable efforts must be taken to prevent children from posting contact information. In certain circumstances and at certain locations, additional warnings and reminders to children must be placed within the website or online service. The participation in games or other online activities may not be conditioned on the disclosure of more information than is necessary. Special limitations are placed on e-mail and the creation of hyperlinks to other websites. Finally, seal participants who e-mail children must also take proactive steps to remind and encourage parents to check and monitor their children's online activities.

In the month that the BBB*OnLine* Privacy program has been in operation, we have already gained much valuable experience. The assessment process involves a lengthy dialog between ourselves and our applicants, and often. we find ourselves learning from each other. For instance, in the process of evaluating the information practices of applicants, we find that we are also educating them on the importance of drafting clear privacy policies that disclose with sufficient specificity what is being collected and how that information is being used. We are talking with applicants about the necessity of providing access to and correction of information, and simultaneously, the importance of having in place verification methods for providing access to only those individuals authorized to obtain it. We are educating applicants on security measures, the many issues that arise in clearly defining the scope of the privacy seal protections, and the best way to protect children's privacy. In this way, we believe we are not only certifying websites that follow the BBB*OnLine* criteria, but also greatly raising the bar by giving applicants the time and guidance needed to make them knowledgeable about the issues surrounding online privacy.

In addition to the assessment process, BBB*OnLine* offers consumers and businesses significant experience in resolving disputes. The BBB system currently runs what is probably the nation's largest consumer-business dispute resolution program, primarily for most of the automobile industry, for whom we are certified as operating state-compliant lemon law programs in those states allowing for state certification; BBB dispute settlement efforts also include 60,000 local business participants; our programs handle more than 30,000 cases a year, using the services of about 5,000 trained volunteer arbitrators, not to mention the hundreds of thousands of informal complaint resolution cases handled by the BBB's every day.

Using BBB's dispute settlement experience, we stand ready to provide consumers with a specialized forum to air and resolve privacy-related disputes (Appendix B). We will accept complaints from both U.S. residents and non-U.S. residents about companies and organizations with posted privacy notices, whose websites or online services are intended to be directed at U.S. residents, that misuse information. Complaints can be about the actions of seal participants and non-seal participants. Companies or organizations that do not cooperate with us in a dispute resolution proceeding can, in turn, be subject to public withdrawal of our seal and/or referral to the appropriate government agency.

Free, convenient, and speedy dispute resolution by trained professionals ensures that consumers have a simple and effective way to have their concerns addressed. Consumers can contact the BBB*OnLine* Dispute Resolution Intake Center via e-mail, telephone call or by simply following our online complaint directions located on our web site at www.bbbonline.org/consumers/drguide.html. As remedies, consumers can seek to have the information which was submitted online used only in

a manner consistent with the company's published privacy policy and/or the consumer can seek to have inaccurate information corrected. BBB*OnLine* may also require corrective action in the form of a change in a seal participant's online privacy policies or practices if, based on the evidence in the case, it finds such action to be required to avoid recurrences of the same complaint.

The BBB*OnLine* dispute resolution process is designed to deliver consumer satisfaction. The first step will be to encourage a business and the consumer to resolve a complaint between the two parties. If this fails, BBB*OnLine* will step in to help, providing a consumer-friendly process to resolve the complaint. An appeal process to an impartial panel is also available providing neutral expertise in the privacy arena. Indeed, we have been fortunate to recruit Andrew Strenio, a former Commissioner of the Federal Trade Commission, to be Chair of our appeals board. Businesses that repeatedly violate their own policies will have their seal revoked, and as previously mentioned, they will be publicly identified and the most serious or frequent offenders will have the violations reported to the proper government authority. The Better Business Bureau system has a long history of cooperation with regulatory authorities and the BBB*OnLine* Privacy Program will continue this collaboration to promote trust and confidence on the Internet.

Seal participants are required to provide information within their privacy policy on how to contact BBB*OnLine* in order to ensure ease of access to the complaint resolution system.

Each participant in the BBB*OnLine* Privacy Program agrees to cooperate with BBB*OnLine* in verification of their compliance with eligibility requirements. BBB*OnLine* may itself, or through an independent third party designated by BBB*OnLine,* conduct random compliance reviews (online, onsite, or otherwise) of one or more eligibility requirements on BBB*OnLine's* own initiative or in response to complaints from individuals or other third parties. By conducting surprise audits on program participants, we will be able to keep the importance of privacy issues at the forefront of online business practices and create a significant deterrence to noncompliance.

If, as a result of a random review or other third party information, BBB*OnLine* finds the organization not to be in compliance with any of our eligibility requirements, we may decide to pursue a complete review of all of the eligibility requirements in order to allow BBB*OnLine* to retain confidence in the organization's continued eligibility to participate in the program. In addition, if the organization is merged, acquired by or consolidated with another company, it must inform BBB*OnLine,* which will require review of the circumstances surrounding the merger, consolidation or acquisition to determine whether the organization must requalify or provide additional information for use of the seal.

We have designed our program to have serious and effective consequences for noncompliance. In our dispute resolution process we will publish decisions so that the public will be able to monitor resolution of complaints about violations of privacy policies. Our complaint resolution process will also keep statistics which will help us identify patterns of improper information practices and instances of non-compliance which we can use to monitor and enforce our program requirements. Of course we will only publish the name of the company complained about, protecting the consumer complainant's identity from disclosure. An important feature of our dispute resolution process is that it will not be binding on the consumer, so consumers will be free to exercise available judicial remedies in addition to the remedies offered by BBB*OnLine.*

The Privacy Seal Program has been officially "open for business" for only one month. In this brief period of time we have already received over 240 applications and have awarded 13 seals. The response has been impressive and more applications are coming in everyday. The assessment process is a very thorough process that forces companies to carefully evaluate, and in some cases change, their entire data collecting and processing practices, online and off-line. The process goes well beyond the posting of a privacy policy.

A study led by AT&T Research Labs released last week came to the conclusion that the combination of a privacy policy and a seal from a well known organization, like the Better Business Bureau, significantly raised people's confidence when they were asked to provide personal information online (www.research.att.com/projects/privacystudy/). In fact, of the respondents that were unsure or said that they would not provide personal information to receive free pamphlets and coupons at a site related to a favorite hobby:

- 48 percent said they would be more likely to provide it if there was a law that prevented the site from using the information for any purpose other than processing the request,

- 28 percent said they would be more likely to provide it if the site only had a privacy policy,
- and 58 percent said they would be more likely to provide it if the site had both a privacy policy and a seal of approval from a well known organization such as the Better Business Bureau

BBB's 100 percent brand name recognition and its 86 year history in self-regulation allows us to provide a program that can make a difference.

Online privacy is often mentioned as one of the biggest concerns keeping consumers from engaging in e-commerce. The online privacy issue has become such a hot issue that many businesses are now starting to respond. As evidenced in our program, it is not only the large businesses that are exercising self-regulation.

Many of the applications we have received have come from small to medium sized businesses. The BBB*OnLine* Privacy Seal Program was intentionally priced so that all companies could apply (Appendix C). The only item keeping a company from participating in the program should be its inability to meet the eligibility requirements; price should not be a factor. The World Wide Web is made up of hundreds of thousands of websites, most of which are not large companies. In order for self-regulation to work it must be accessable to the majority of web marketers, large and small companies alike. Indeed, now that we are open for business we are engaging in an aggressive outreach effort to reach as wide a business audience as possible. For example, we recently entered into a co-marketing arrangement with the American Electronic Association to educate their 3,000 plus members about good privacy principles and the BBB*OnLine* Privacy Program.

BBB*OnLine* plans a comprehensive outreach effort for consumer education. We have approached consumer advocacy groups about joint efforts and hope to use our website to provide educational materials on helping consumers protect their privacy online.

Though we just launched the Privacy Seal Program, it is our hope that as the program grows and as consumer awareness and education increases we will have been able to make the online marketplace a safer place to negotiate for all. We want to thank the Committee for your attention and hope that you share in our enthusiasm for the tremendous progress already made.

I am available to answer any questions you may have.

APPENDIX

Appendix A:

BBB*OnLine* Privacy Program Compliance Assessment Document

Appendix B:

BBB*OnLine* Privacy Program Dispute Resolution Process

Appendix C:

BBB*OnLine* Privacy Program Dispute Resolution (Flow Charts)

Appendix D:

BBB*OnLine* Privacy Program Seal Price Schedule

Appendix E:

BBB*OnLine* Privacy Program Selected Media Coverage

APPENDIX A

BBB*OnLine*® Privacy Program
Compliance Assessment Questionnaire

Applicants for a BBB*OnLine* Privacy Seal must complete this questionnaire. You must answer every question except where the instructions with respect to a question(s) indicate that an answer is not necessary. If a question asks you to provide a description or explanation of your organization's practices or mechanisms, you may attach a copy of a document that provides such information instead of writing in a description or explanation. If you are responding to a question by attaching a document, please note that fact and the name of the document in the space provided for the answer to the question and note the question number on the face of the document.

It is recommended that you review the Eligibility Criteria before you begin work on the questionnaire. We have also prepared a list of the business documents that you may need to refer to in working through the application, Application and Compliance Assessment Questionnaire Guide. If you have questions about this assessment document, you can contact us at bbbprivacy@cbbb.bbb.org.

If you are using a disk copy or hard copy of the questionnaire, please forward the completed questionnaire and any associated documents to:

BBB*OnLine* Privacy Program
4200 Wilson Boulevard
Suite 800
Arlington, VA 22203-1838

If you are completing the questionnaire online and wish to include documents in your response, please send the documents by email to bbbprivacy@cbbb.bbb.org. Be sure to include your **confirmation number** in the subject line of your email message.

We will notify you as soon as we have completed our review of your submission. During that review, we will be verifying the answers to some questions by spot checks of your website(s) or online service(s) and we may also need to contact you (the individual completing this assessment) for further information or clarification.

Submission Information

Name, address, email address and phone number of individual completing this assessment:

Date of submission of completed questionnaire and any associated documents:

SECTIONS OF THIS QUESTIONNAIRE

A. General Organizational Information
B. Privacy Notice: General
C. Information Collection
D. Information Use and Transfer
E. Choice/Consent
F. Data Security
G. Access
H. Relationship of Site to Children
I. Prior Verifiable Parental Consent
J. Children's Privacy Notices
K. Parental Access
L. Information Collected As Part Of A Child's Activity
M. When Prior Verifiable Consent Is Not Required
N. Hyperlinking To A Page Belonging To Another Website Or Online Service
O. Additional Statements To Parents

A. General Organizational Information

A.1. Name of the organization applying for the seal:

Help screen

Generally, the applicant for a seal should be the organization that offers information, products, or services from a website(s) or online service(s) and that is responsible for the representations made with regard to the privacy practices of the website(s) or online service(s) whose privacy practices will be governed by the seal. It may also be the parent of such organization. It may be a partnership, sole proprietorship, corporation (for profit or not for profit), a joint venture, association or any other legal entity authorized to maintain a website or an online service. If the organization that so controls the site or service is a corporate subsidiary or other distinct legal entity that is part of a larger entity, that subsidiary or distinct legal entity may apply for the seal on its own. Conversely, in such situations, the corporate parent of the subsidiary or the larger entity that encompasses the smaller may apply for the seal. A "corporate parent" is an entity that owns or controls a majority (50.1% or more) of the stock of another corporate organization.

A.2. Identify the operating website(s) or online service(s) whose practices will be governed by the seal being applied for (list the URL(s) for the identified website(s) or online service(s)).

Help screen

Give the domain name for any website, and/or for any online service without a website, that will be covered by the seal. List the URL(s) for the homepage of the identified website(s) and for the entry point for any identified online service(s) without a website.

To be eligible for the seal, a website or online service must be operating, that is, must be online.

In addition, the site or service must be directed at residents of the U.S., its territories or possessions (U.S. residents). In determining whether a site or service is directed at U.S. residents, BBBOnLine will consider the applicant's statement of its intent. It will also evaluate and weigh objective indications of that intent such as whether there is: advertising aimed at U.S. customers; actual sales knowingly made to U.S. customers generated from the web or online activity; email directed to US residents; contracts to provide services to U.S. customers; actual presence in the U.S. of an office or plant; and other substantial contacts with the U.S., such as a sales force, suppliers and distributors in the U.S., and use of a web server located in the U.S.. A site or service does not have to be directed exclusively to U.S. residents to qualify as directed to U.S. residents.

An applicant can treat an entire domain as one website or treat subdomains/subdirectories and/or a collection of pages within a domain that are dedicated to a specific purpose as separate websites. An online service is any Internet Service Provider (ISP), content provider, or other service, which provides, or provides access to, online activities.

A.3. Does this application cover more than one website or online service?

Yes/no

A.4. Does this application cover all websites or online services of the applicant? If your answer is yes, go to Question A.9.

Yes/no

[Please go to A.9 if yes]

Help screen

An applicant may choose to exclude from the application websites operated by its corporate subsidiaries or operating divisions or websites that it has dedicated to discrete readily identifiable product lines or other specific purposes. It may wish to take this approach, for example, if a particular part of its business is subject to specific regulatory requirements that it wishes to be handled through the regulatory procedures rather than its privacy policy and BBB*OnLine*, if it is not ready to implement an online privacy policy for a particular business, or if it hosts within its website a website dedicated to another purpose and controlled by a person or entity without any affiliation to the organization.

An applicant that wishes to make such an exclusion must clearly disclose the fact of the exclusion in its privacy notice. In addition, the effect of such exclusions, must not be confusing or misleading to the public that is relying on the display of a BBB*OnLine* seal on the organization's website. For example, an exclusion of a majority of divisions or product lines would be confusing, and the better alternative for an organization making such a choice would be to apply for the seal on individual divisions or product line websites rather than rely on the top-level website as the applicant. The possibility of confusion also can be eliminated by alerting individuals to the significance of following any link from a covered site or service to an excluded site or service.

A.5. If you answered no to A.4, are there any links from the covered website(s) or online service(s) to any of the website(s) or online service(s) that are excluded from this application? If your answer is no, go to Question A.8.

Yes/no

[Please go to A.8 if no]

A.6. If you answered yes to A.5, are there alerts at all such links to advise individuals that they are moving outside the seal covered website or online service when they follow the link. If your answer is no, go to Question A.8.

Yes/no

[Please go to A.8 if no]

A.7. If you answered yes to A.5, please provide a list of URLs for a representative sample of the pages on which such links appear and then go to Question A.9.

[Please go to A.9 if question is answered]

A.8. If you answered no to A.5 or A.6, identify any corporate subsidiaries, operating divisions or discrete readily identifiable product lines of the organization whose websites are not covered by this application or any other subsites of the covered website(s) not covered by this application.

A.9. Is use of the covered website(s) or online service(s) limited to residents of the U.S.? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If your answer is no, go to Section B.

Yes/no

[Please go to Section B if no]

Help screen

Where an organization restricts use of a website to U.S. residents because the nature of the site makes it suitable only for U.S. residents, it may exclude non U.S. residents from the site's privacy policies under certain conditions. A site would be considered suitable only for U.S. residents where the organization a) maintains sister sites for non U.S. residents or uses the site to market goods that cannot be ordered by persons residing outside the U.S., and b) prominently displays a notice independent of its privacy notice stating that use of the site is restricted to U.S. residents at the site's homepage, and on every page on which information is collected. In addition, the site's privacy notice must include notice of such limitation.

A.10. If you answered yes to A.9, is there a notice to this effect prominently posted on the homepage(s) for the website(s) or the entry page(s) for the online service(s) and on each page where information is collected?

Yes/no

Help screen

A site can not restrict its privacy policies to U.S. residents unless it prominently displays a notice independent of its privacy notice stating that use of the site is restricted to U.S. residents at the site's homepage, and on every page on which information is collected. It must also meet the other conditions noted in the help screen for A.9.

A.11. If you answered yes to A.9, please provide an explanation of the limits and the reasons for such limits. (If this question is applicable to more than one website or online service, please answer by site or service.)

B. Privacy Notice: General

B.1. Does each covered website or online service have a privacy policy in effect for the website or service?

Help screen for "covered website(s) or online service(s)"

Covered websites or online services are the websites or online services that will be governed by the seal – the sites or services identified in response to Question A.2. *[Note: There is a help screen for "covered website(s) or online service(s)"]*

B.2. Please provide the name(s) and position(s), or the position title(s), of the individual(s) charged with the responsibility for implementation and oversight of the privacy policy for the covered website(s) or online service(s). (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

Since a privacy policy is not self-implementing, assurance that the information practices prescribed in the policy are being followed depends on there being some assignment of responsibility for implementation and oversight of the policy.

B.3. Summarize the steps the organization has taken to implement the privacy policy for each covered website(s) or online service(s) (e.g., incorporated the policy in its personnel and training materials). (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

B.4. Is a statement of this privacy policy (i.e., a privacy notice) either posted on or accessible through a hyperlink from the homepage of any covered website(s) and the entry point(s) of any covered online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

An organization's privacy notice must be easy to find. At the very least, the privacy notice must be accessible by a link from (i) the organization's homepage or entry point and (ii) at every subsequent point where the organization elicits individually identifiable information online through means other than passive data collection. The terms of the privacy notice are very important because they substantially determine an individual's understanding of how information will be used and what steps the individual may choose to take to protect his or her privacy.

B.5. If you answered yes to B.4, list the URL(s) for the website(s) homepage(s) or the entry point(s) of the online service(s).

B.6. Does the privacy notice(s) explain how an individual can contact the organization to express questions or concerns about the organization's privacy policies and practices? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

The explanation should include contact information, e.g., a phone number or email address, that will lead a person with a complaint about the treatment of his/her information to a person responsible for the receipt of such complaints without undue delay. In most cases, this means that a person calling during normal business hours should be able to speak to such a person during that first call or by the end of the next business day. This does not require that the complaint be resolved in that timeframe but simply that the individual have an opportunity to make an initial contact with a person authorized to take information about the complaint and begin the process of resolving it. An example of the form that such explanation might take is included in the help screen for the following question.

B.7. Does the privacy notice(s) note the availability of the BBB*OnLine* dispute resolution mechanism? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

This provision does not require a detailed discussion of the dispute resolution process. For example, a statement such as the following would be acceptable for purposes of both this provision and B.6:

If you have any questions, concerns, or comments about our privacy policies or practices, we would like to know what they are so we can address them. Please contact us at 1 000 000 0000. In addition, we participate in BBB*OnLine*. Further information about that program is available at www.bbbonline.org/privacy.

B.8. If you answered no to Question A.4, does the privacy notice(s) disclose the fact that the seal application does not cover all of the organization's websites or online services? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

B.9. If you answered no to Question A.4 and no to Question A.5 or A.6, does your privacy notice(s) identify the website(s) or online service(s) that are not covered? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

B.10. If you answered yes to Question A.11, is the inapplicability of the privacy policy to non U.S. residents disclosed in the privacy notice? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

The privacy notice must disclose the effect of limitation of the site to U.S. residents.

C. Information Collection

C.1. Does the covered website(s) or online service(s) collect individually identifiable information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen for "covered website(s) or online service(s)"

Covered websites or online services are the websites or online services that will be governed by the seal – the sites or services identified in response to Question A.2.

Help screen for "individually identifiable information"

The data covered by the BBBOnLine seal program is limited to "individually identifiable information" and "prospect information" in an online or electronic commerce environment.

"Individually identifiable information" means information that:

- when associated with an individual can be used to identify him or her;
- is elicited from the individual by the organization's online website through active or passive data collection; and
- is retrievable by the organization in its ordinary course of business.

The term "individually identifiable information" does not include:

- information that the organization did not obtain online from the individual;
- information that the website cannot retrieve by the individual's name, email address or similarly specific identifier in its ordinary course of business;
- IP addresses that identify only the computer used to access the network rather than individuals and are linked to that computer only for a particular online session identifying a different subscriber during a different online session; or
- navigational or clickstream data (passively collected data) unless it is linked to a name or similarly specific identifier

The term "individually identifiable information" is intended to encompass information that, when associated with an individual, can be used to identify him or her, for instance, email addresses and other information that is compiled and linked to an email address. Account, billing, and online transactional information are examples of individually identifiable information. Information need not be unique to be considered capable of identifying an individual. Consequently, addresses, telephone numbers, and dates of birth constitute individually identifiable information. Information must be capable of identifying an individual, however. Consequently, data generated by passively browsing an online site (also known as navigational or clickstream data) does not constitute individually identifiable information unless it is linked to a name, email address, or similar information that identifies an individual.

In addition, the information must be information collected by the organization from the individual online. Information received by the organization, online or offline, that was collected online from the individual by others (who are not making the collection as an agent or contractor of the organization) is not itself individually identifiable information in the hands of the organization. This includes, for example, public records information in the possession of the organization that was collected online from the individual by the government agency.

Generally, information submitted by an individual acting in her/his business capacity (such as a company purchasing agent) that meets the above definition is individually identifiable information. It is not individually identifiable information only if (i) the individual is acting solely in a business capacity, and (ii) such submissions are specifically excluded from the protection provided by the site's or online service's online privacy policy, and (iii) the privacy notice for the site or service clearly states that information submitted solely in a business capacity is not covered by the site's or service's privacy or security policies. In addition, to avoid improper exclusions, the organization must use effective means to determine that information is submitted solely in a business capacity.

The definition of prospect information is covered under Question C.5.

Information is retrievable in the ordinary course of business only if it can be retrieved by taking steps that are taken on a regular basis in the conduct of the business with respect to that information or that the organization is capable of taking with the procedures it uses on a regular basis in its conduct of its business. Information is not retrievable in the ordinary course of business if retrieval would impose an unreasonable burden.

C.2. Is information submitted by an individual acting solely in a business capacity excluded from the scope of the privacy and security policies of the covered website(s) or online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If your answer is no, go to Question C.5.

Yes/no

Help screen

Generally, information submitted by an individual acting in her/his business capacity (such as a company purchasing agent) that meets the definition of individually identifiable information is individually identifiable information and therefore can not be excluded from the scope of the privacy and security policies of the site(s) or service(s). It is not individually identifiable information only if (i) the individual is acting solely in a business capacity, and (ii) such submissions are specifically excluded from the protection provided by the site's or online service's online privacy policy, and (iii) the privacy notice for the site or service clearly states that information submitted solely in a business capacity is not covered by the site's or service's privacy or security policies. In addition, to avoid improper

exclusions, the organization must use effective means to determine that information is submitted solely in a business capacity.

C.3. If you answered yes to C.2, is the fact of this exclusion clearly stated in the privacy notice for the covered website(s) or online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

C.4. If you answered yes to C.2, please describe the means used to determine whether information is submitted solely in a business capacity.

C.5. Does the covered website(s) or online service(s) collect prospect information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen for "prospect information"

"Prospect information" means information that:

- when associated with an individual can be used to identify him or her;
- is elicited by the organization's online website through active data collection from an individual other than the individual identified by the information; and
- is retrievable by the organization in its ordinary course of business.

The term "prospect information" does not include:

- information that the organization did not obtain online from an individual; or
- information that the website cannot retrieve by the individual's name, email address or similarly specific identifier in its ordinary course of business.

Information is retrievable in the ordinary course of business only if it can be retrieved by taking steps that are taken on a regular basis in the conduct of the business with respect to that information or that the organization is capable of taking with the procedures it uses on a regular basis in its conduct of its business. Information is not retrievable in the ordinary course of business if retrieval would impose an unreasonable burden.

C.6. Is the privacy notice posted at or accessible through a hyperlink from every page in all of the covered websites or online services? If your answer is yes, go to C.11.

Yes/no

[Please go to C.11 if yes]

C.7. If your answer to C.6 is no, is the privacy notice posted at or accessible through a hyperlink from every page in the covered website(s) or online service(s) where individually identifiable information or prospect information is collected? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen for "individually identifiable information or prospect information"

Information is individually identifiable information or prospect information if it was collected by the organization online from an individual (including information collected through passive means), is information that when associated with an individual can be used to identify him or her and is retrievable by the website(s) or online service(s) by the individual's name, email address or similarly specific identifier in its ordinary course of business.

The fact that information is submitted in a business capacity does not exclude it from the category of individually identifiable information unless the organization has provided, under the processes referenced in C.2 through C.4 above, for the exclusion of information submitted solely in a business capacity.

Information is retrievable in the ordinary course of business only if it can be retrieved by taking steps that are taken on a regular basis in the conduct of the business with respect to that information or that the organization is capable of taking with the procedures it uses on a regular basis in its conduct of its business. Information is not retrievable in the ordinary course of business if retrieval would impose an unreasonable burden.

Help screen for "collected"

For purposes of this question, "collected" means collected through means other than passive data collection.

C.8. If you have a written protocol for establishing forms for collection of individually identifiable information and/or collection of prospect information on the covered website(s) or online service(s) that requires that the privacy notice for the site(s) or service(s) be posted on or accessible through a hyperlink from any web page or online service location where such information is collected, please attach it. (If the application covers more than one website or online service, please attach material for each site or service for which such protocol exists.)

Help screen for "collected"

For purposes of this question, "collected" means collected through means other than passive data collection.

C.9. For each site or service for which you attached material in response to C.8, please list the URL(s) for a representative sample of the web page(s) within the covered website(s) or for the location(s) within the covered online service(s) where individually identifiable information or prospect information is collected. If you have attached material for all covered websites or online services, go to Question C.11.

Help screen for "collected"

For purposes of this question, "collected" means collected through means other than passive data collection.

C.10. If there are any covered website(s) or online service(s) for which you did not attach material in response to C.8, please list the URL(s) for the web page(s) within those website(s) or for the location(s) within those online service(s) where individually identifiable information or prospect information is collected. (If this question is applicable to more than one website or online service and the answer is not the same for all, answer by website or online service.)

C.11. Describe the specific types of individually identifiable information or prospect information collected at the covered website(s) or online service(s). (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

Please list all types of individually identifiable information or prospect information collected either actively or passively. For example, include personal identifiers like names and email addresses, information about websites that have been visited where linked to email addresses or other specific identifiers, information about purchases, information about preferences. If the application covers more than one website or online service, list the information by website or online service.

Information is individually identifiable information or prospect information if it was collected by the organization online from an individual (including information collected through passive means), is information that when associated with an individual can be used to identify him or her and is retrievable by the website(s) or online service(s) by the individual's name, email address or similarly specific identifier in its ordinary course of business.

The fact that information is submitted in a business capacity does not exclude it from the category of individually identifiable information unless the organization has provided, under the processes referenced in C.2 through C.4 above, for the exclusion of information submitted solely in a business capacity.

Information is retrievable in the ordinary course of business only if it can be retrieved by taking steps that are taken on a regular basis in the conduct of the business with respect to that information or that the organization is capable of taking with the procedures it uses on a regular basis in its conduct of its business. Information is not retrievable in the ordinary course of business if retrieval would impose an unreasonable burden.

C.12. Does the privacy notice(s) state the types of individually identifiable information and prospect information that are being collected at the covered website(s) or online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

An important function of a privacy notice is to inform individuals about what information is being collected about them with sufficient specificity for them to know and understand what that information is so that they can make informed choices about the use of the website(s) or online service(s).

C.13. Do other organizations collect individually identifiable information or prospect information as a result of transacting business directly with the individual at the organization's website(s) or online service(s)? If your answer is no, go to Section D. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

[Please go to D if no]

Help screen

For purposes of this question, "other organizations" means any organization other than the applicant unless it is an agent or contractor of the applicant. In addition, if the organization has excluded any sites operated by corporate subsidiaries or operating divisions or sites dedicated to discrete readily identifiable product lines from the application (Section B), those subsidiaries, operating divisions or discrete product lines would be "other organizations" for purposes of this question.

This question covers situations in which other entities collect information as the result of activity at the organization's site(s) or service(s), for instance, communication providers, merchants, or electronic payment providers. For example, where a consumer purchases goods from a merchant hosted on an organization's site, the merchant may be the only entity that collects and uses the individually identifiable information.

C.14. If you answered yes to Question C.13, is the fact that other organizations collect such information at the website(s) or online service(s) disclosed in the privacy notice for the affected website(s) or online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

With the seamlessness of the online environment, it is reasonable for an individual to assume that the organization that is the seal recipient is the only entity that is capable of collecting individually identifiable information at its site, and that the organization will identify in its privacy notice the types of third parties to whom it may distribute the information. If other entities collect individually identifiable information as the result of activity at its site, the organization's privacy notice must notify individuals of this fact and that the consumer should contact the other organization directly for further information on its use of customer information.

A site is not responsible for the information practices of other organizations that transact business directly with the individual at the site. For example, where an individual uses a credit card to pay for a purchase at the site, the site is not responsible to the individual for the information practices of the credit card company. The site is only responsible for informing the consumer that he or she should contact the credit card company directly for further information on its use of customer information. The privacy policy or the credit card company, with whom the individual has a direct and separate relationship, governs the company's privacy practices.

D. Information Use and Transfer

D.1. Describe what each of the types of individually identifiable information described in the answer to Question C.11, is used for. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

For example, indicate whether a specific type of information is used for communication back to the individual, updates on services and benefits, marketing to the individual, transfers to third parties, etc. If all the information described in C.11 is used for the same purposes, you may list "all" as the types of information to which the uses apply. If the only use made of some or all of the information described in C.11 is to complete the transaction for which the information is submitted, you should state that in your response with respect to that information.

D.2. Describe what each of the types of prospect information described in the answer to Question C.11, is used for. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

D.3. For each of the types of individually identifiable information or prospect information described in the answer to Question C.11 above, state (by site or service, if the application covers more than one and the answer is not the same for all) whether the information is ever shared with:

a) Agents or contractors?

b) Corporate affiliates **not** governed by a common privacy policy and a common data security policy?

c) Unaffiliated third parties?

Help screen for (a)

For purposes of this questionnaire, an agent is a person other than an employee or an organization that performs services for the applicant under an express or implied agreement and is subject to the applicant's control or right to control the manner and means of providing the service. A contractor is a person or entity who, as part of an independent business, becomes obligated to provide goods and/or services to the applicant.

Help screen for (b)

This question refers to a corporate affiliate of the governing organization of the website or service, the organization that offers information, products, or services from the covered website(s) or online service(s) and is responsible for the representations made with regard to the privacy practices of the website(s) or online service(s) whose privacy practices will be governed by the seal, whether that governing organization or its parent is the applicant. For purposes of this questionnaire, an affiliate of the governing organization is an organization that has the power to control the governing organization or that can be controlled by the governing organization or an organization that is controlled by the same entity that controls the governing organization. Elements of control include, in part, interlocking management or ownership, shared facilities and equipment, common use of employees.

An affiliate is governed by a common privacy policy and common data security policy if (i) its privacy policy and data security are established by an entity that controls it and the governing organization of the covered website(s) or online service(s) and that promulgates the same privacy policy and data security policies for both affiliates, or (ii) it controls the governing organization and promulgates the same policies for itself and that organization.

Help screen for (c)

Unaffiliated third parties include any person or entity that is not an employee or corporate affiliate and not acting in its capacity as an agent or contractor.

D.4. If you answered "yes" to Questions D.3(b) or (c) or both, does the privacy notice of the covered website(s) or online service(s) inform individuals of this sharing of the information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen for "covered website(s) or online service(s)"

Covered websites or online services are the websites or online services that will be governed by the seal – the sites or services identified in response to Question A.2.

D.5. Does the privacy notice for each of the covered websites or online services state all of the uses described in response to Questions D.1 and D.2 with respect to that website or online service? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

A website or online service must disclose in its privacy notice all of the types of uses and transfers of individually identifiable information then applicable to the individually identifiable information being collected (actively or passively) at the site or service. It is not necessary for each use to be spelled out in detail but there must be sufficient information for the individual to be reasonably informed as to what uses will be made of the information. For example, "We use this information to better understand your needs and provide you better service" is not a sufficient disclosure of an intent to use the information to market to the individual. In addition, if the site(s) or service(s) transfers any of this information to unaffiliated third parties or corporate affiliates not governed by a common privacy policy for the marketing purposes of those parties, that fact must be specifically stated in its privacy notice.

D.6. Does the organization enhance or merge individually identifiable information or prospect information collected at the covered website(s) or online service(s) with data from third parties for purposes of marketing products or services to the individual? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.). If your answer is no, go to Question D.8.

Yes/no

[Please go to D.8 if no]

Help screen for "third parties"

For purposes of this question "third parties" means any unaffiliated third parties and corporate affiliates not governed by a common privacy policy.

D.7. If your answer to Question D.6 is yes for any website or service, does the privacy notice for the affected website(s) state this practice? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

Because enhancing or merging individually identifiable information or prospect information collected at the site or service with data from third parties for purposes of marketing products or services to the individual may affect an individual's expectations, the privacy notice should disclose this practice.

D.8. If you answered yes to Questions D.3(b) or D.3(c), describe the processes that are in place with respect to each affected website or online service to try to ensure that unaffiliated third parties or corporate affiliates not governed by a common privacy policy that receive individually identifiable information from you are aware of your privacy and security policies applicable to such data and that they will take reasonable precautions to similarly protect such information. (If this question is answered by your response to B.3, you may respond by simply indicating that.)

Help screen

Organizations should take reasonable steps to assure that unaffiliated third parties or corporate affiliates not governed by a common privacy policy to which they transfer individually identifiable information are aware of these security practices, and that such parties also take reasonable precautions to protect any transferred information.

D.9. If you answered yes to Question D.3(a), are agents and contractors for each of the affected websites or online services required to agree to honor the organization's privacy and security policies in their handling of individually identifiable information and prospect information? (If this question is answered by your response to B.3, you may respond by simply indicating that.)

Help screen

Agents and contractors who will have access to individually identifiable information and prospect information must agree to hold the information in confidence and not make any use of it except to carry out the services they are performing for the organization. This agreement can be in whatever form serves this purpose. For example, it may be a specific commitment to follow the organization's privacy and security policies or a commitment to treat the information as proprietary information of the organization.

E. Choice/Consent

E.1. If you answered yes to Question C.1, does the organization restrict its use of individually identifiable information collected at a covered website or online service to the uses specified in the privacy notice for the website or service at the time the information is collected, those uses or transfers that are necessarily incident to carrying out such a specified use and other uses specifically permitted under BBB*OnLine* Privacy Program policies? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online

service.) If your answer is yes or the question is inapplicable to you because you do not collect individually identifiable information, go to Question E.3.

Yes/no

[Please go to E.3 if yes]

Help screen

Covered websites or online services are the websites or online services that will be governed by the seal – the sites or services identified in response to Question A.2.

Uses or transfers of individually identifiable information that are specified in the notice at the time the information is collected are related uses. Uses necessarily incident to carrying out a use disclosed in the privacy notice also constitute related uses or transfers. For example, a site's transfer of individually identifiable information to agents or contractors to process orders is necessarily incident to rendering a service permitted by the privacy notice.

In addition, there are three uses that are permitted whether or not they are specified in the notice. The first is where the organization is required by law to divulge the information, for example, in response to a court order or a subpoena or the requirements of agency rules. The second exception is where the information is used for research activities, including the production of statistical reports, where the individually identifiable information is not published, divulged, or used to contact the individuals. The third is in situations where the information is shared in the context of a business transaction such as a divestiture pursuant to a pledge of confidentiality under which the recipient agrees to use the information for no purpose other than carrying out the transaction. You should answer yes to the above question if you restrict use of the information to related uses and the three permitted uses noted.

E.2. If your answer to Question E.1 is no, does the organization provide individuals with an opportunity to opt out or otherwise prohibit any unrelated use of their information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen for "unrelated use"

Any use of information that was not permitted in the privacy notice in effect at the time the information was collected, and is not a use necessarily incident to carrying out a use that was disclosed in the privacy notice at that time, is unrelated to the purpose for which the information was collected. Organizations intending to use individually identifiable information for an unrelated use, other than a use that falls within one of the three exceptions noted in the help screen for E.1 above, must provide the affected individuals with the opportunity to opt out or otherwise prohibit these new uses of the information about them.

E.3. If you answered yes to Question C.5, does the organization use prospect information for its own marketing to the individual? (If the application covers more than one website or online service and the answer is not the same for all, list the information by website or online service.) If your answer is no, go to Question E.6.

Yes/no

[Please go to E.6 if no]

E.4. If you answered yes to Question E.3, does the covered website(s) or online service(s) at which prospect information used for internal marketing is collected offer individuals who submit information a choice as to whether to receive marketing information from the organization? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If your answer is no, go to Question E.6.

Yes/no

[Please go to E.6 if no]

E.5. If you answered yes to Question E.4, do you offer the individuals who are the subject of prospect information a choice as to whether to receive marketing information from you? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

Individuals who are the subject of prospect information should not be treated any less favorably than individuals who submit information themselves. Consequently, if a site or service offers individuals submitting information a choice as to whether to receive marketing information from it, it should provide the same choice to "prospect." This requirement can be met by offering the "prospect" an opportunity to opt out of or opt in to further marketing at the time of the organization's first marketing contact with such individual.

E.6. If you answered yes to Question C.5, does the organization restrict its use of prospect information to carrying out the purposes for which the information was submitted, its own marketing use and other uses specifically permitted under BBB*OnLine* Privacy Program policies?

Help screen

Generally, prospect information may not be used for any purposes other than the purposes for which it was submitted and marketing to the individual by the organization that collected the information. The only exceptions to this rule are where i) the organization is required by law to divulge the information, ii) it is used in research activities, including the production of statistical reports, where the individually identifiable information is not published, divulged, or used to contact the individuals, or iii) it is shared in the context of a business transaction such as a divestiture pursuant to a pledge of confidentiality under which the recipient agrees to use the information for no purpose other than carrying out the transaction. Prospect information may not be transferred in any way to an unaffiliated third party or corporate affiliate not governed by a common privacy policy for their marketing purposes.

E.7. If you answered yes to Question D.3(b) or D.3(c), does the organization rent, sell, exchange, or in any manner provide individually identifiable information to such outside parties for their marketing purposes? (If the application covers more than one website or online service and the answer is not the same for each, answer by website or online service.) If your answer is no, go to E.13.

Yes/no

[Please go to E.13 if no]

Help screen for "outside parties"

An outside party is any unaffiliated third party or corporate affiliate not governed by a common privacy policy as those terms are defined for purposes of Question D.3.

E.8. If you answered yes to Question E.7, list the URL(s) for the page(s) within the website(s) or the locations within the online service(s) where the organization provides individuals with the opportunity to bar this transfer of information by opting out or not opting in. (If the application covers more than one website or online service, list the information by website or online service.)

Help screen

Regardless of the disclosure an organization makes in the privacy notice about its practice of renting, selling, or exchanging or in any way providing individually identifiable information for marketing purposes, an organization that makes such transfers to outside parties must provide individuals with the ability to prevent these transfers in connection with individually identifiable information about them. Providing individuals with an opt out will satisfy this requirement. It can also be satisfied by an opt in or, when technological tools that enable individuals to make choices about transfers become available, by the use of such tools as are determined by BBB*OnLine* to satisfy its requirements.

E.9. If you answered yes to Question E.7, does the website provide a technological tool (e.g., P3P) that enables the individual to make choices about the transfers to outside parties for marketing purposes? (If the application covers more than one website or online service, answer by website or online service.) If your answer is no, go to Question E.12.

Yes/no

[Please go to E.12 if no]

Help screen

The acceptability of such a tool as an alternative to opt outs or opt ins will be determined by BBB*OnLine* when the tool becomes available.

E.10. If you answered yes to Question E.7, what is the tool?

E.11. If you answered yes to Question E.7, list the URL(s) for the page(s) within the website(s) or the location(s) within the online service(s) where individuals can learn about this tool? (If the application covers more than one website or online service, list the information by website or online service.)

E.12. Does the privacy notice inform individuals of the choices available to them for preventing the transfer of individually identifiable information about them collected at the covered website(s) or online service(s) to outside parties for marketing purposes? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

E.13. Does the organization condition the granting of access to certain areas of the covered website(s) or online service(s) on the individual's disclosure of information that it links to individually identifiable information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If the answer is no, go to Section F.

Yes/no

[Please go to Section F if no]

E.14. If your answer to E.13 is yes with respect to any covered website or online service, does the organization -- either in its notice on such website or service, or at the point or time of collection on such website or service -- inform individuals of the consequences of refusing to provide such information?

Yes/no

F. Data Security

F.1. Does the privacy notice for each covered website or online service contain a statement about the organization's commitment to data security with respect to information collected on the site or service? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

Covered websites or online services are the websites or online services that will be governed by the seal – the sites or services identified in response to Question A.2.

Although an organization is not required to provide a description in its privacy notice(s) of the data security measures it undertakes to protect individually identifiable information, it is required to take appropriate data security measures and to inform the public that such measures are in place by a statement in its privacy notice. The security measures must include physical security measures such as doors, locks, etc., electronic security and managerial controls that limit the potential for misuse of information by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by the organization's collection and use of the data.

F.2. Is the computer equipment in which individually identifiable information or prospect information collected at the covered website(s) or online server(s) is stored, and any other copy of such information, located in a secure physical environment that includes doors, locks, etc. to keep unauthorized individuals from accessing the information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

Copies include hard copies and electronic copies in any form.

An organization is required to take appropriate data security measures to protect individually identifiable information and prospect information collected online. These measures must include physical security measures such as doors, locks, etc., electronic security and managerial controls that limit the potential for misuse of information by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by the organization's collection and use of the data.

F.3. Please describe in general terms the security measures taken by the organization to ensure the security needed to prevent unauthorized electronic access to individually identifiable information and prospect information collected at its covered website(s) or online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

An organization is required to take appropriate data security measures to protect individually identifiable information and prospect information collected online. These measures must include physical security measures such as doors, locks, etc., electronic security and managerial controls that limit the potential for misuse of information by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by the organization's collection and use of the data.

F.4. Does the website(s) or online service(s) collect health care information, social security numbers, financial transaction information or other sensitive information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If no, go to Question F.7.

Yes/no

[Please go to F.7 if no]

F.5. If you answered yes to F.4, is encryption used when transferring or receiving all such information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

For information being transferred between the individual and the organization, the use of encryption satisfies that appropriate security measures have been taken. While not required in all instances, encryption must be used for the most sensitive of information including the transfer of health care information, social security numbers, and financial transactional information (e.g. credit card number).

F.6. If you answered yes to F.5, please list the URL(s) for the page(s) within the website(s) or the location(s) within the online service(s) that use encryption when transferring or receiving such information? (If the application covers more than one website or online service and the information is transferred or received on more than one, list the URLs by website or online service.)

F.7. Does the organization maintain written security policies to protect individually identifiable information and prospect information from unauthorized individuals? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

In order to demonstrate managerial controls, the organization must maintain written security polices to protect individually identifiable information and prospect information from unauthorized individuals. Employees who routinely have access to such information must receive adequate training and must be familiar with the organization's information practices.

F.8. Please describe how you ensure that only authorized persons have physical or electronic access to individually identifiable information and prospect information and how you determine who is authorized. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If this question is answered with respect to electronic security by your response to F.3, you may respond to that part of this question by simply indicating that.

F.9. Please describe the training with respect to the organization's information practices that is provided to the personnel within the organization who interact with or otherwise have access to individually identifiable information collected at the website(s) or online service(s)? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If this question is answered by your response to B.3, you may respond by simply indicating that.

Help screen

In order to demonstrate managerial controls, the organization must maintain written security polices to protect individually identifiable information and prospect information from unauthorized individuals. Employees who routinely have access to such information must receive adequate training and must be familiar with the organization's information practices.

F.10. Does the organization maintain logs to help implement its physical security and electronic security procedures? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

Logs are a necessary part of an adequate security system as they are needed to assure that data is properly tracked and only authorized individuals are getting access to the data.

G. Access

G.1. Does the organization maintain individually identifiable information or prospect information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If the answer is no, go to Section H.

Yes/no

[Please go to Section H if no]

Help screen

An organization is not required to set up any new systems to maintain information or to maintain individually identifiable information or prospect information beyond a time when it no longer serves the organization's purposes.

Information is individually identifiable information or prospect information if it was collected by the organization online from an individual (including information collected through passive means), is information that when associated with an individual can be used to identify him or her and is retrievable by the website(s) or online service(s) by the individual's name, email address or similarly specific identifier in its ordinary course of business.

The fact that information is submitted in a business capacity does not exclude it from the category of individually identifiable information unless the organization has provided, under the processes referenced in C.2 through C.4 above, for the exclusion of information submitted solely in a business capacity.

Information is retrievable in the ordinary course of business only if it can be retrieved by taking steps that are taken on a regular basis in the conduct of the business with respect to that information or that the organization is capable of taking with the procedures it uses on a regular basis in its conduct of its business. Information is not retrievable in the ordinary course of business if retrieval would impose an unreasonable burden.

G.2. Describe the mechanism(s) the organization has in place to help assure the accuracy of the individually identifiable information or prospect information that it maintains. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

Organizations must take reasonable steps to assure that the individually identifiable information and prospect information they collect is accurate, complete, and timely for the purposes for which it is used. They must also establish appropriate processes or mechanisms so that factual inaccuracies in individually identifiable information may be corrected.

G.3. Are the mechanisms described in response to G.2 described in the privacy notice(s) for each of the covered websites or online services?

Yes/no

Help screen for "covered website(s) or online service(s)"

Covered websites or online services are the websites or online services that will be governed by the seal – the sites or services identified in response to Question A.2.

G.4. Describe the mechanism(s) the organization has in place to make available to individuals upon reasonable request the individually identifiable information or prospect information it maintains with respect to the individual? Please include in the description a statement of any terms with respect to frequency limits or fees. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

An organization must establish a mechanism whereby, upon request and proper identification of the individual, it makes available to the individual the individually identifiable information or prospect information it maintains with respect to the individual. The information subject to this requirement tends to be, but is not limited to, (i) account or application information, for example, name, address, and level of service subscribed to, and (ii) billing information and similar data about transactions conducted online, for example, date and amount of purchase, and credit card account used.

If an organization can not make information that it maintains available because it can not retrieve the information in the ordinary course of business, it must provide the individual with a reference to the provisions in its privacy notice that discuss the type of data collected, how it is used, and appropriate choices related to that data, or provide the individual with materials on these matters that are at least as complete as the information provided in the privacy notice.

Organizations have substantial flexibility in deciding how best to make the individually identifiable information or prospect information available to the individual. For example, an organization may choose the form in which it discloses this information to the individual. Monthly statements from banks and credit card companies are examples of appropriate mechanisms to satisfy this disclosure obligation, even though they may reveal more than the individually identifiable information that the individual submitted to the organization online. The organization also determines the reasonable terms under which it will make such information available such as limits on frequency and the imposition of fees. Frequency limits that require intervals of more than a year between requests and/or fees of more than $15 for a response to an annual request would not be reasonable except in extraordinary circumstances.

G.5. Does the privacy notice(s) inform individuals of the opportunity to request this information about themselves? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Yes/no

Help screen

Sites or services must inform individuals that this opportunity exists.

G.6. Explain in general terms the method used to authenticate the identity of the individual requesting disclosure? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

The organization must take reasonable steps to assure itself that the individual to whom it makes individually identifiable information available is the same person from whom the organization collected the information and that the individual to whom it makes prospect information available is the person who is the subject of the information.

G.7. Describe the mechanisms the organization has in place to allow individuals to correct factual inaccuracies to the individually identifiable information or prospect information that it maintains with respect to the individual. (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If the answer to this question is covered by your response to G.2, you may answer this question by simply stating that fact.

Help screen

Upon the request of an affected individual, an organization must correct factual inaccuracies in the individually identifiable information it maintains about him or her, if the information will be communicated to others or used for substantive decision making. There is no obligation to ascertain the accuracy of such factual information, unless the individual's request includes information that suggests the likelihood of a factual inaccuracy. The organization chooses the form of the showing that an individual must make to suggest the likelihood of a factual inaccuracy in the individually identifiable information that it maintains.

G.8. Does the privacy notice(s) inform individuals of this opportunity to correct factual inaccuracies to the individually identifiable information or prospect information?

Yes/no

Help screen

Sites or services must inform individuals that this opportunity exists.

G.9. Explain in general terms the method used to authenticate the identity of the individual requesting an opportunity to correct information? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.)

Help screen

The organization must take reasonable steps to assure itself that the individual who is requesting correction of individually identifiable information is the same person from whom the organization collected the information and that the individual requesting correction of prospect information is the person who is the subject of the information.

H. Relationship of Site to Children

H.1. Is any portion of the covered website(s) directed to children under the age of 13? If your answer is yes, go to Section I.

Yes/no

[Please go to section I if yes]

Help screen for "directed to children"

A website or portion of a website is "directed to children" if the website or portion appears to be intended to attract children under 13. The subject matter, visual content, age of models, language, advertising and the context in which the site or service appears are all relevant to this determination along with any other pertinent characteristics of the site or service. For example, an online general interest bookstore or compact disc store will not be considered to be directed to children, even though children visit the site. If a general interest site has a special area for children, then that portion of the site will be considered to be directed to children.

H.2. Do you collect individually identifiable information at a covered website(s) or online service(s) from any particular visitor actually known to be under the age of 13? (If the application covers more than one website or online service and the answer is not the same for all, answer by website or online service.) If your answer is yes, go to Section I. If your answers to this question and the preceding question are no, you have completed the Questionnaire.

Yes/no

[Please go to Section I if yes]

Help screen

Although websites or online services, or portions thereof, that are not directed to children are not required to carry the children's seal, any site or service at which individually identifiable information is collected from a visitor actually known to be under the age of 13 is required to answer the Assessment Questions in Section I and the following sections. For these purposes, knowing a visitor's grade in school or other information that indicates an age of under 13 is actual knowledge that the visitor is under 13.

Applicants are deemed to 'actually know' they are collecting information from particular visitors under the age of 13 when applicants request the visitor's age or age category, segregate visitors on the website or online service by age, structure the website or online service in such a way as to determine age, or in some other way act in an affirmative manner which would enable an applicant to know or learn which particular visitors are under the age of 13 and then collect information from such visitors.

An applicant is not required to answer the Questions in Section I and the following sections when an applicant receives unsolicited information indicating age from a visitor and the applicant did not affirmatively elicit such information.

BBB*OnLine*® Privacy Program
Children's Supplemental Assessment Questionnaire

The following requirements apply to applicants that operate websites, online services, or portions thereof, that are directed to children under the age of 13, or collect individually identifying information from particular visitors actually known to be under the age of 13.

Help screen

The children's seal requirements operate as supplements to those already contained in the main Compliance Assessment Questionnaire.

These requirements are based upon the guidelines of the Council of Better Business Bureaus' Children's Advertising Review Unit (CARU), the industry standards suggested by the Online Privacy Alliance (OPA) and the Children's Online Privacy Protection Act of 1998 (COPPA), which authorizes the Federal Trade Commission (FTC) to promulgate regulations protecting children's online privacy.

Since the FTC is still considering its rules regarding COPPA, these requirements may change over time to reflect applicable FTC rules.

In addition to the questions asked in the main Compliance Assessment Questionnaire, applicants that operate websites or online services, or portions thereof, that are directed to children under the age of 13 will need to answer the questions contained in the children's supplemental assessment questionnaire, comply with the substantive requirements of the BBB*OnLine* children's seal program, and carry the children's seal.

Applicants with websites or online services, or portions thereof, that are not directed to children, but at which individually identifiable information is collected from any particular visitor actually known to be under the age of 13, will not be required to carry the children's seal if they so choose, but such applicants must answer the children's supplemental assessment questionnaire and comply with the substantive requirements of the BBB*OnLine* children's seal program.

Applicants are deemed to 'actually know' they are collecting information from particular visitors under the age of 13 when applicants request the visitor's age or age category, segregate visitors on the website or online service by age, structure the website or online service in such a way as to determine age, or in some other way act in an affirmative manner which would enable an applicant to know or learn which particular visitors are under the age of 13 and then collect information from such visitors.

Note that there may be circumstances when an applicant may actually know the age of a particular visitor is under 13, but does not know the visitor's precise age.

An applicant is not required to answer the children's supplemental assessment questionnaire or comply with the substantive requirements of the BBB*OnLine* children's seal program when an applicant receives unsolicited information indicating age from a visitor and the applicant did not affirmatively elicit such information. For example, the children's seal requirements would not apply to a general interest website that makes no efforts to determine age and yet receives an unsolicited post on one of its bulletin boards which indicates a visitor's email address and also that visitor's age as being under 13.

DEFINITIONS

Child or **Children** means individual(s) under the age of 13.

Best Efforts means commercially reasonable efforts that discourage children from publicly posting contact information and minimize the likelihood they will do so. These efforts may include online warnings and reminders to children, monitoring, efforts to educate parents, and the use of available technological tools.

Contact Information means offline and online contact information.

Collection and **Collection Practices** includes the practice of associating passive information with a name or similarly specific identifier.

Disclosure, or **Disclose** means the release of individually identifiable information collected from a child by an applicant; as well as the making of individually identifiable information collected from a child publicly available by an applicant by any means including public posting, the Internet, a home page, a pen pal service, an electronic mail service, a message board, or a chat room. It is not a disclosure where such information is provided to a person who provides support for the internal operations of an applicant if that person does not disclose or use that information for any other purpose.

Disclosure Practices are those actions, intended actions, or features of a site or online service that disclose individually identifiable information. For example, a disclosure practice would include a feature of a website or online service that automatically makes online contact information publicly available in identifiable form through message boards or chat rooms.

Individually Identifiable Information means information that:

- when associated with an individual can be used to identify him or her;
- is elicited from the individual by a website or online service through active or passive data collection; and
- is retrievable by the organization in its ordinary course of business.

The term "individually identifiable information" does not include:

- information that the organization did not obtain online from the individual;
- information that the website or online service cannot retrieve by the individual's name, email address or similarly specific identifier in its ordinary course of business;
- IP addresses that identify only the computer used to access the network rather than individuals and are linked to that computer only for a particular online session identifying a different subscriber during a different online session; or
- passive information unless it is associated with a name or similarly specific identifier.

Non-Identifying Name means an alias, first name, nickname, initials, or other alternative to a child's full name.

Online Contact Information means email addresses or similar identifiers that permit direct contact with a person online.

Parent means parent or legal guardian.

Passive Information means navigational and tracking data, browser file data, cookie and click stream data, and any other kind of behavioral data an applicant may gather from a child.

Prior Verifiable Parental Consent means that before individually identifiable information is collected from a child, an applicant must make reasonable efforts in light of available technology to ensure that:

1) a parent of a child receives notice of the applicant's individually identifiable information collection, use, and disclosure practices, and

2) parental authorization is obtained for the collection, use, and disclosure of individually identifiable information and subsequent use of that information as described in the applicant's notice.

Prominently And Readily Accessible Notice can include prominently and readily accessible hyperlinks that directly lead to a notice.

Secondary Entry Points are those parts of a website or online service that are held out to receive Web traffic other than an applicant's home page or entry point. Secondary entry points include all advertised URLs and points on any applicant's website or online service to which an approved outside hyperlink directly leads.

Website Or Online Service Directed To Children is any website, online service, or portion thereof, with apparent objective characteristics demonstrating a structure intended to attract children. These objective characteristics include, but are not limited to: subject matter, visual content, age of models, language, advertising, and surrounding context. For example, an online general interest bookstore by itself will not be considered directed to children, even though children may visit that website. However, if an online general interest bookstore has a special area set aside for children containing apparent objective characteristics demonstrating a structure intended to attract children, then that portion of the website will be considered directed to children. Where an applicant does not already request a children's seal, the BBB*OnLine* Staff reserves the right to require applicants and those portions of their website or online service to comply with the children's privacy seal requirements if all or part of the website or online service to be covered by a seal is found directed to children.

I. PRIOR VERIFIABLE PARENTAL CONSENT

Note: The questions in section **I** apply in all circumstances except where the requirements to obtain prior verifiable parental consent have been specifically excepted (see **M** below).

I1. THE COLLECTION, USE, OR DISCLOSURE OF INFORMATION

Help screen

Except where not required (see **M** below), an applicant must obtain prior verifiable parental consent for the collection, use, or disclosure of children's individually identifiable information.

I1.1 If you collect children's individually identifiable information, do you obtain prior verifiable parental consent?

I1.2 If you use children's individually identifiable information, do you obtain prior verifiable parental consent?

I1.3 If you disclose children's individually identifiable information, do you obtain prior verifiable parental consent?

I2. THE ABILITY TO POST AND DIRECTLY COMMUNICATE WITH OTHERS

Help screen

An applicant must obtain prior verifiable parental consent before giving children the ability to publicly post or otherwise distribute individually identifiable information, or when children will be given the ability to otherwise communicate directly with others.

I2.1 If you give children the ability to publicly post or otherwise distribute individually identifiable information, do you obtain prior verifiable parental consent?

I2.2 If you give children the ability to otherwise directly communicate with others, do you obtain prior verifiable parental consent?

I3. DESCRIPTION OF PRIOR VERIFIABLE PARENTAL CONSENT

I3.1 Please thoroughly describe how you obtain prior verifiable parental consent, as mentioned in questions **I1.1**, **I1.2**, **I1.3**, **I2.1**, and **I2.2**

Help screen

Prior verifiable parental consent means that before individually identifiable information is collected from a child, an applicant must make reasonable efforts in light of available technology to ensure that:

1) a parent of a child receives notice of the applicant's individually identifiable information collection, use, and disclosure practices, and

2) parental authorization is obtained for the collection, use, and disclosure of individually identifiable information and subsequent use of that information as described in the applicant's notice.

Acceptable efforts to obtain verifiable parental consent can take several forms, as long as they are reasonable efforts in light of available technology.

For example, current acceptable means of obtaining verifiable parental consent include the use of a consent form that can be downloaded and printed for the parent to fill out, sign, and send back to the applicant by fax or mail; or credit card verification where the card number is verified in the course of a transaction or by other reliable means.

Conversely, unacceptable means of obtaining verifiable parental consent would be sole reliance on notices without further interaction between the applicant and parent that simply encourage a child to ask for permission, or the sole use of email without also having a reliable device in place to ensure that the parent actually authored the email granting consent. For instance, consent obtained from a supposedly parental email address would be unacceptable when the address is provided by the child and children can easily establish multiple email addresses.

J. NOTICE

J1. PRIVACY NOTICE

Help screen

Applicants must provide a prominent and readily accessible privacy notice on the applicant's homepage or entry point, and those points on which an applicant requests individually identifiable information.

In addition to the notices required in the main Compliance Assessment Questionnaire, applicants' privacy notice will also address:

- All collection practices which involve the association of passive information with a name or similarly specific identifier.
- All disclosure practices in addition to any third party distributions of individually identifiable information; and
- How a parent can access his/her child's individually identifiable information as discussed in **K**.

J1.1 In addition to the notice requirements contained in the main Compliance Assessment Questionnaire, does your privacy notice also address:

a) all collection practices which involve the association of passive information with a name or similarly specific identifier,

b) all disclosure practices in addition to any third party distributions of individually identifiable information; and

c) how a parent can access his/her child's individually identifiable information?
(See Question K below).

J1.2 Does this notice or direct link to a notice, appear in a prominent and readily accessible manner on:

a) your homepage or entry point,

b) those points at which you request individually identifiable information?

J2. ADDITIONAL STATEMENTS TO CHILDREN

Help screen

Even when prior verifiable parental consent is obtained, it remains important to provide enough information for children to make their own informed decisions about whether or not to disclose information. Therefore, in certain circumstances, applicants are also required to direct additional statements to children in language they can easily understand. It is the intention of the BBB*OnLine* Privacy Program to afford applicants flexibility in meeting these requirements, as long as these informative statements effectively communicate their meaning to children at the points and times they are required.

The privacy notice is primarily intended to create a tool for parents, and therefore does not necessarily need to be in language easily understood by a child.

However, if the applicant uses a privacy notice to fulfill some or all of its "additional statements to children" requirements, and thus creates a "dual-use" situation where both parents and children are relying on the same notice, then the privacy notice must appear where those additional statements to children are required to appear, and those parts of the privacy notice which are addressed to children must appear prominently within the notice and be in language easily understood by a child.

For example, a privacy notice may begin as a "Note To Kids" and then continue as a "Note To Parents."

Alternately, if an applicant creates a privacy notice without using language easily understood by a child, it must also provide separate statements where these additional statements to children are required. These statements should be prominent and readily accessible, and written in language easily understood by a child. All notices and statements, regardless of language or placement, must be consistent with each other.

There are five circumstances where an applicant is required to provide additional effective statements to children. These are:

1) when passive information is collected and associated with a name or similarly specific identifier,

2) when individually identifiable information is requested,

3) when a child has been granted the ability to post information,

4) when a child is contacted by email, and

5) when a child activates a hyperlink leading to a page residing on part of another website or online service that is directed to children or at which individually identifiable information is collected from particular visitors

actually known to be under the age of 13; if that is the device the applicant has chosen when offering hyperlinks to other websites or online services. [See **N** below].

J2.1 If you collect passive information that is associated with a name or similarly specific identifier, do you also provide:

a) a prominently placed statement or direct link to that statement,

b) appearing on your homepage or entry point, and every secondary entry point,

c) written in language easily understood by a child

d) that explains what passive information is being collected?

Help screen

When applicants collect passive information that is, or will be, associated with a name or similarly specific identifier, in addition to obtaining prior verifiable parental consent, applicants must also provide a statement to children explaining what passive information is collected. This statement may be incorporated into a privacy notice or appear separately, but must be in language easily understood by a child, and appear in a prominent and readily accessible manner on the applicant's homepage or entry point and every secondary entry point.

J2.2 If you collect passive information associated with a child's name or similarly specific identifier, please provide a list of the URLs for every secondary entry point to your website or online service.

J2.3 After acquiring prior verifiable parental consent, if individually identifiable information is requested of a child, do you also provide:

a) a prominently placed statement or direct link to that statement,

b) appearing where you request such information,

c) written in language easily understood by a child

d) that explains why the information is being requested, and

e) that states whether you intend to disclose the information.

Help screen

When applicants request individually identifiable information, in addition to obtaining prior verifiable parental consent, applicants must also provide a statement to children where individually identifiable information is requested explaining why the information is being requested and whether the applicant intends to disclose the information. This statement may be incorporated in the general privacy notice or appear separately, but must be in language easily understood by a child and appear in a prominent and readily accessible manner.

J2.4 After acquiring prior verifiable parental consent granting a child the ability to post information, do you also:

a) make best efforts to prohibit a child from posting contact information, and

b) remind children to use non-identifying names, such as aliases, first names only, nicknames, initials, or other alternatives to full names in any activity which will involve public posting?

Help screen

When applicants grant children the ability to post information, in addition to obtaining prior verifiable parental consent, applicants must also make best efforts to prohibit a child from then posting contact information and to remind children to use non-identifying names, such as aliases, first names only, nicknames, initials, or similar alternatives to full names in any activity which will involve public posting. "Best efforts" means commercially reasonable efforts that discourage children from publicly posting contact information and minimize the likelihood they will do so. These efforts may include online warnings and reminders to children, monitoring, efforts to educate parents, and the use of available technological tools.

J2.5 If children are able to post on your website or online service, and you make best efforts to prevent children from posting contact information and to remind children to use non-identifying names in any activity that involves public posting, please provide a list of URLs at which any efforts you make online are demonstrated.

J2.6 Please describe any other online efforts you make to prevent children from posting contact information and to remind children to use non-identifying names in any activity that involves public posting.

J2.7 Please describe any offline efforts you make to prevent children from posting contact information and to remind children to use non-identifying names in any activity that involves public posting.

J2.8 If your website or online service uses a system that corresponds "screen names" to email addresses or some other method of direct communication, are your best efforts with regards to screen names carried out by providing at a minimum:

a) a prominently placed notice or direct link to a notice,

b) appearing at the time or immediately before a child can engage in activities that would disclose screen names,

c) written in language easily understood by a child,

d) that explains that the child's contact information will be publicly disclosed by engaging in that activity?

Help screen

When applicants use systems that correspond "screen names" to email addresses or other methods of direct online communication, these best efforts with regards to screen names will mean providing a statement to children at the time or immediately before a child can engage in any activity that would disclose a screen name explaining to the child that the child's online contact information will be publicly disclosed by engaging in such activities. This statement may be incorporated in the privacy notice or appear separately, but must be in language easily understood by a child and appear in a prominent and readily accessible manner.

J2.9 If you communicate more than once with a child by email, do you also include an opportunity with each mailing for the child to choose by return email to discontinue receiving mailings?

Help screen

When an applicant communicates with a child by email, there shall also be an opportunity with each mailing for the child to choose by return email to discontinue receiving mailings. This requirement does not apply if an applicant is responding directly only once inside the scope of a child's specific request and the information is not used to recontact the child nor maintained in retrievable form. (See **M** below).

K. PARENTAL ACCESS

K1. PARENTAL ACCESS

K1.1 If a child has provided individually identifiable information to your site or online activity, and a parent subsequently makes a request and provides proper identification, do you provide to that parent:

a) a description of the specific types of individually identifiable information you collected from the child,

b) an opportunity at any time to refuse further use or maintenance of the individually identifiable information in retrievable form, or future online collection of individually identifiable information from that child, and;

c) a means that is reasonable under the circumstances for the parent to obtain any individually identifiable information collected from that child.

Help screen

An applicant must provide, upon request of a parent whose child has provided individually identifiable information to that website or online service, upon proper identification of that parent:

1) a description of the specific types of individually identifiable information collected from the child by that applicant,

2) the opportunity at any time to refuse to permit the applicant's further use or maintenance in retrievable form, or future online collection, of individually identifiable information from that child at that website or online service, and

3) a means that is reasonable under the circumstances for the parent to obtain any individually identifiable information collected from that child.

If a parent refuses to permit an applicant's further use or maintenance in retrievable form, or future online collection, of individually identifiable information from that parent's child, applicants may, if they so choose, terminate service provided to that child.

Please refer to the provisions contained in the main assessment questionnaire explanatory materials for additional discussion of an applicant's obligation to provide individual access to individually identifiable information.

L. INFORMATION COLLECTED AS PART OF A CHILD'S ACTIVITY

L1. INFORMATION COLLECTED AS PART OF A CHILD'S ACTIVITY

L1.1 Do you avoid conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more individually identifiable information than is reasonably necessary to participate in such activity?

Help screen

Applicants shall not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more information than is reasonably necessary to participate in such activity.

L1.2 Please provide a specific list of all the types of individually identifiable information you find reasonably necessary for a child to disclose in order to participate for all of your activities.

M. WHEN PRIOR VERIFIABLE CONSENT IS NOT REQUIRED

M1. RESPONDING TO A CHILD'S SPECIFIC REQUEST ON A ONE-TIME BASIS

M1.1 If you collect online contact information from children which is used solely to respond to a child's request on a one-time basis, do you:

a) avoid using such information for any purpose beyond the scope of the child's request?

b) not maintain such information in retrievable form?

Help screen

Applicants are not required to obtain prior verifiable parental consent in the case of online contact information collected from a child that is used only to respond directly to a child's specific request on a one-time basis if such information is not used to recontact the child, and such information is not maintained in retrievable form by the applicant after responding.

M2. RESPONDING TO A CHILD'S SPECIFIC REQUEST MORE THAN ONCE

M2.1 If you collect online contact information from children that is used solely to respond to a child's request, and that response requires more than a single contact, do you:

a) avoid using such information for any purpose beyond the scope of the child's request?

b) not maintain such information in retrievable form?

M2.2 If you collect online contact information from children that is used solely to respond to a child's request, and that response requires more than a single contact, before the second contact do you also provide direct parental notification that contains:

a) the type of online contact information which was collected from the child,

b) the purposes for which it is to be used, and

c) an opportunity for the parent to request that you:

i) make no further use of the information, and

ii) not maintain the information in retrievable form.

Help screen

Applicants are not required to obtain prior verifiable parental consent in the case of online contact information collected from a child that is used to respond directly to a child's specific request more than once if:

1) such information is not used to recontact the child beyond the scope of that request,

2) such information is not maintained in retrievable form by the applicant after the last response, and

3) before such information is used after the initial response to the child, applicants provide:

a) direct parental notice of the type of online contact information collected from the child,

b) the purposes for which it is to be used, and

c) an opportunity for the parent to request that the applicant make no further use of the information and that it not be maintained in retrievable form.

M2.3 Please submit an example of such parental notice.

M3. INFORMATION COLLECTED TO OBTAIN PARENTAL CONSENT OR PROVIDE NOTICE

M3.1 If you request the name or online contact information about either a parent or child that is used solely for obtaining parental consent or providing notice, do you also remove such information in retrievable form if parental consent is not obtained after a reasonable time?

Help screen

Applicants are not required to obtain prior verifiable parental consent for the collection, use, or disclosure of children's individually identifiable information in the case of a request for the name or online contact information of a parent or child that is used for:

1) the sole purpose of obtaining parental consent, or

2) providing notice; and

3) where such information is not maintained in retrievable form by the applicant if parental consent is not obtained after a reasonable time.

For example, an applicant need not obtain prior verifiable parental consent in order to request a child's first name and the parent's email address in order to send the parent the direct notice required when responding to a child's request more than once.

M3.2 Taking into consideration the nature of your website or online activity, as well as the methods you use for obtaining parental consent or providing notice, please explain what you consider a reasonable time.

M4. INFORMATION OBTAINED TO PROTECT THE SAFETY OF A CHILD

M4.1 If you request a child's name or online contact information to the extent reasonably necessary to protect the safety of a child participating on your website or online service, do you also:

a) only use that information for the purpose of protecting the child's safety,

b) not use that information to recontact the child for any other purpose,

c) not disclose that information on your website or online service, and

d) use reasonable efforts to provide a parent:

i) notice of the name and online contact information collected from the child,

ii) notice of the purpose for which it is to be used, and

iii) an opportunity for the parent to request that you make no further use of the information and that it no longer be maintained in retrievable form?

Help screen

Applicants are not required to obtain prior verifiable parental consent for the use of a child's name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the website or online service if:

1) such information is only used for the purpose of protecting such safety;

2) such information is not used to recontact the child for any other purpose,

3) such information is not disclosed on the website or online service, and

4) the applicant uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the applicant make no further use of the information and that it not be maintained in retrievable form.

For example, if a child was revealing instances of family abuse in a monitored chat room or bulletin board, it would be possible for the applicant to request and retain the name and online contact information of that child in order to help, but only to the extent necessary to protect the safety of the child. This information could only be used when the applicant believes the safety of a child participating on that website or online service is threatened, and the applicant must make reasonable efforts to provide direct parental notification.

M5. INFORMATION OBTAINED TO PROTECT THE WEBSITE OR ONLINE SERVICE

M5.1 Are all other instances when children's individually identifiable information may be collected, used, or disclosed without obtaining prior verifiable parental consent limited to only those instances necessary to:

a) protect the security or integrity of your website or online service,

b) take precautions against liability,

c) respond to judicial process, or

d) the extent permitted under other provisions of law or regulation, to provide information to law enforcement agencies, or for an investigation of a matter related to public safety?

Help screen

Applicants are not required to obtain prior verifiable parental consent for the collection, use, or dissemination of such information by an applicant necessary to:

1) protect the security or integrity of its website,

2) take precautions against liability,

3) respond to judicial process, or

4) the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

N. HYPERLINKING TO A PAGE BELONGING TO ANOTHER WEBSITE OR ONLINE SERVICE

Note: If applicants create or maintain hyperlinks leading to other websites or online services, applicants must follow at <u>least one</u> of the two information practices inquired into below.

Information Practice #1

N1. PROVIDING A STATEMENT TO CHILDREN WHEN A HYPERLINK IS ACTIVATED

N1.1 If you create or maintain hyperlinks leading to other websites or online services, do you provide a prominent statement to children that appears when a hyperlink leading to another website or online service is activated?

N1.2 Does this statement appear until the child closes the notice or clicks through to continue?

N1.3 Does the statement explain in language easily understood by a child,

a) that the child is leaving your website or online service,

b) that other websites or online services may use different information practices, and

c) that the child needs a parent's permission before answering any information gathering questions?

Help screen

Applicants must provide a prominent statement to children that appears when a hyperlink to another website or online service is activated. This statement must appear until the child closes that particular statement or clicks through to continue.

This statement must explain in language easily understood by a child that the child is leaving the applicant's website or online service, other websites or online services may use different information practices, and that parental permission is needed before a child can answer information gathering questions.

For example, an acceptable statement may appear as a pop-up window, an alert box, or an intermediate page and say: "You are now leaving the [applicant] site. Please remember that other sites may treat things they learn about you differently. Get your parent's permission before you type-in anything about yourself."

N1.4 Please provide an example of this statement or provide a URL where this statement is demonstrated on your website or online service.

Information Practice #2

N2. AVOIDING NONCOMPLIANT WEBSITES OR ONLINE SERVICES

N2.1 If you create or maintain hyperlinks leading to other websites or online services, do you avoid hyperlinking to the page of another website or online service residing on the part of another website or online service that is directed to children [or that collects individually identifiable information from particular visitors actually known to be under the age of 13] when that page:

a) fails to obtain prior verifiable parental consent for the collection, use, or disclosure of a child's individually identifiable information except as described in **M** [above].

b) fails to provide a prominent and readily accessible privacy notice if the page is also the homepage or entry point,

c) fails to provide reasonable parental access to learn the specific types of individually identifiable information collected by that page from that parent's child, and to provide the parent an opportunity to remove such information from retrievable form, or

d) is identified to you through credible notice as being noncompliant with any of these core standards, or is identified as part of a website or online service in substantive noncompliance with the BBB*OnLine* children's seal program. Such notice includes notice from the BBB*OnLine* Privacy Program.

Help screen

Applicants must not hyperlink to a page residing on part of another website or online service directed to children [or that collects individually identifiable information from particular visitors actually known to be under the age of 13] when:

a) the page fails to obtain prior verifiable parental consent for the collection, use, or disclosure of a child's individually identifiable information except as described in **M** [above],

b) the page fails to provide a prominent and readily accessible privacy notice if the page is a homepage or entry point,

c) the page fails to provide reasonable access to a parent to learn the specific types of individually identifiable information collected from that parent's child by that page, and to provide the parent an opportunity to remove such information from retrievable form; or

d) the page is identified through credible notice to the applicant as being noncompliant with any of these core standards, or is identified as part of a website or online service in substantive noncompliance with the BBB*OnLine* children's seal program. Such notice includes notice from the BBB*OnLine* Privacy Program.

N2.2 Do you have the necessary provisions in place whereby you can eliminate hyperlinks when you determine a page fails to meet the core standards listed above, or you receive credible notice that the page resides on a website or online service that is noncompliant with the substantive requirements of the BBB*OnLine* children's seal program?

O. ADDITIONAL STATEMENTS TO PARENTS

O1. REMINDING AND ENCOURAGING PARENTS TO CHECK AND MONITOR

O1.1 If you communicate with children by email, do you also take steps to remind and encourage parents to regularly check and monitor their children's use of email and other online activities?

Help screen

When an applicant chooses to communicate with a child by email, the applicant must also take steps to remind and encourage parents to regularly check and monitor their children's use of email and other online activities.

For example, applicants may take part in online or offline parental education efforts; or include such reminders in billing statements, the prior verifiable consent process, and the direct parental notice process.

O1.2 Please provide a list of URLs at which any efforts you take online to remind and encourage parents are demonstrated.

O1.3 Please describe any other online efforts you take to remind and encourage parents.

O1.4 Please describe any offline efforts you take to remind and encourage parents.

APPENDIX B

BBB*OnLine*® Privacy Program
Dispute Resolution Process Procedures
Privacy Policy Review Service And Privacy Review Appeals Board

General Procedures
Effective February 11, 1999

PART 1 OVERVIEW 52

1.1 GENERAL 52
1.2 PARTIES TO PPRS/PRAB PROCEEDINGS 52
1.3 PARTIES' WAIVER OF SUBPOENA RIGHTS AND OF LIABILITY CLAIMS 52
1.4 CONFIDENTIALITY OF PPRS AND PRAB FILES 52
1.5 PARTIES' TREATMENT OF INFORMATION RECEIVED DURING THE PROCESS 52
1.6 REFERRALS TO GOVERNMENT AGENCIES AND SEAL COMPLIANCE REVIEW BECAUSE OF FAILURE TO PARTICIPATE 53

PART 2 ELIGIBLE COMPLAINTS 54

2.1 SUMMARY 54
2.2 PERSONAL ELIGIBILITY 54
2.3 ELIGIBLE CLAIMS 54
2.4 INELIGIBLE CLAIMS 54
2.5 AVAILABLE REMEDIES 55
2.6 INTAKE FUNCTION 55
2.7 HANDLING OF GENERAL INQUIRIES 55
2.8 HANDLING OF POTENTIAL COMPLAINTS 55
2.8.1 Inquiry into status of potential respondent 55
2.8.2 Inquiry into prior attempt to resolve the complaint 55
2.8.3 Verifying identity of complainant and representative 56
2.8.4 Forwarding potential complaint to complaint review process 56

PART 3 DISPUTE RESOLUTION BY THE BBB*ONLINE* PRIVACY POLICY REVIEW SERVICE (PPRS) 57

3.1 FUNCTION OF PPRS IN DISPUTE RESOLUTION PROCESS 57
3.2 INFORMATION IN PPRS PROCEEDINGS 57
3.2.1 Information required to sustain a complaint 57
3.2.2 When information may be treated as confidential 57
3.2.3 Providing a nonconfidential summary of confidential information 57
3.3 PPRS COMPLAINT REVIEW 57
3.4 REPLIES AND RESPONSES TO COMPLAINT AND REQUESTS FROM PPRS 58
3.4.1 Respondent's answer to a complaint 58

3.4.2 Complainant's reply to respondent's answer 58
3.4.3 Respondent's response to a reply 58
3.4.4 PPRS request for additional information or comments 58
3.4.5 Conferences 58
3.4.6 Failure to answer a complaint 59
3.4.7 Late filings 59
3.5 PPRS CASE RECORD 59
3.6 PPRS DECISIONS 60
3.6.1 PPRS's "Findings, Recommendations and Conclusions" 60
3.6.2 Finalizing a decision where corrective action is not required 60
3.6.3 Finalizing a decision where corrective action is required 60
PART 4 APPEALS TO PRAB 61
4.1 DISCRETIONARY APPEALS 61
4.2 RIGHT TO APPEAL 61
4.3 FILINGS IN AN APPEAL 61
4.3.1 Filing an appeal 61
4.3.2 Filing a cross appeal 61
4.3.3 Explanation of reasons for appeal 61
4.3.4 Late filings 61
4.4 FORWARDING OF CASE RECORD TO THE PARTIES 62
4.5 RECORD ON APPEAL 62
4.6 APPOINTMENT OF PRAB CHAIR AND MEMBERS 62
4.6.1 Appointment of the Chair 62
4.6.2 Appointment of PRAB members 62
4.7 APPOINTMENT OF PANEL 62
4.7.1 Appointment by Chair 62
4.7.2 Eligibility of panelists 62
4.7.3 Composition of panel 63
4.8 PROCEDURE OF PANEL 63
4.9 PANEL DECISIONS 63
4.9.1 Issuance of a decision 63
4.9.2 Noncompliance with a decision 64
PART 5 CLOSING A CASE 65
PART 6 REPORTING OF PPRS/PRAB ACTIVITY AND PUBLICATION OF DECISIONS 66

Part 1 OVERVIEW

1.1 General

The BBB*OnLine* Online Privacy Program Dispute Resolution Process provides for review of an eligible complaint by the Privacy Policy Review Service (PPRS) of BBB*OnLine*, Inc., (a subsidiary of the Council of Better Business Bureaus, Inc.). In addition, where the complaint is against a company or individual that is a participant in the BBB*OnLine* Privacy Program, there may be an opportunity for a PPRS decision to be appealed to the Privacy Review Appeals Board (PRAB).

1.2 Parties To PPRS/PRAB Proceedings

The parties to a proceeding are:

the complainant, the individual complaining about misuse of information, and
the respondent, the company, organization or individual about whom the complainant is complaining.

A party may designate another individual as a representative during the dispute resolution process under procedures specified by BBB*OnLine*.

1.3 Parties' Waiver Of Subpoena Rights And Of Liability Claims

By participating in a PPRS or PRAB process, the parties agree that they will not subpoena the staff of the Council of Better Business Bureaus, Inc., or BBB*OnLine,* Inc., their Board members, committee members or volunteers, or any records of the PPRS or PRAB proceedings in any subsequent legal proceeding arising out of the matters at issue in the process in which they are participating. They also agree that the Council of Better Business Bureaus, Inc., BBB*OnLine*, Inc. their staffs, Board members, committee members or volunteers shall not be liable for any act or omission in connection with the online privacy dispute resolution process.

1.4 Confidentiality Of PPRS And PRAB Files

PPRS and PRAB shall maintain a record of their proceedings, but a verbatim record is not required. All deliberations, meetings, proceedings and writings of a PPRS reviewer or PRAB panel other than their decisions shall be treated as confidential by the PPRS and PRAB. A PPRS decision, and a PRAB decision in those cases referred to a PRAB panel, are the only permanent records required to be kept as to the basis of a complaint, the issues defined, the facts and information presented, and the conclusions reached by PPRS, or PRAB if it has been involved in the process.

Case materials, other than confidential materials, that are not required to be kept as part of the case record shall be kept for a period of three years. Confidential materials submitted to PPRS shall be returned when PPRS issues its decision in the matter or closes a case without a decision. If submitted to PRAB, they shall be returned or destroyed when the case is closed.

1.5 Parties' Treatment Of Information Received During The Process

By participating in a PPRS or PRAB process, the parties agree that during the course of the process they will treat any information provided to them by the PPRS staff or PRAB panel as information provided exclusively for the purpose of furthering the review and that they will not provide the material to anyone except persons directly involved in the handling of the complaint. If a party violates this agreement, PPRS, or PRAB, may refuse to proceed with the case. The purpose of this right of refusal is to maintain a professional, unbiased atmosphere in which PPRS or PRAB can effect a timely and lasting resolution to a case in the spirit of furthering voluntary self-regulation of online privacy and the voluntary cooperation of the

parties involved. If the party violating the agreement is a respondent, PPRS may refer the matter to the appropriate government agency if appropriate and, if the party is a seal participant, may withdraw or suspend the seal if appropriate.

1.6 Referrals To Government Agencies And Seal Compliance Review Because Of Failure To Participate

When PPRS's preliminary review of a complaint indicates it is an eligible claim submitted by an eligible complainant and the individual or organization complained about indicates directly or indirectly during the PPRS review that it is not willing to participate in the process or a respondent fails to comply or appeal after a PPRS decision requiring corrective action, PPRS, shall refer the matter to the appropriate government agency. If an organization or individual complained about indicates directly or indirectly in the course of a PRAB appeal that it is not willing to participate in the appeal or fails to comply after a PRAB decision requiring corrective action, the PRAB Chair may refer the matter to the appropriate government agency. Reports of such referrals shall be included in the PPRS Reports and may be included in other BBB*OnLine* publications. If the referred organization or individual is a *BBBOnLine* Privacy Program participant, PPRS shall withdraw or suspend the seal. See also, sections 3.4.6, 3.6.3, 4.9.2.

Part 2 ELIGIBLE COMPLAINTS

2.1 SUMMARY

To have a complaint eligible for resolution through the dispute resolution process, the complaining individual must be personally eligible to file a complaint and must have an eligible claim.

2.2 PERSONAL ELIGIBILITY

The individual's complaint must be about:

a) the use of information that identifies himself/herself or identifies another individual that was collected online from him/her, or
the use of information that identifies a child that was collected online from such child when she/he was under the age of 13, or
the use of information that identifies himself/herself that was collected online from another individual; and

b) information that was collected --
by an organization through a website or online service displaying the BBB*OnLine* Privacy Program Seal, or through any other website or online service directed at residents of the U.S., its territories or possessions that displays a statement advising users of the site that privacy safeguards will apply to the information collected from them.

The complainant must be (i) the person who provided the personal information to the organization or individual that collected it and allegedly misused it, (ii) the parent or legal guardian of the person in the case of information collected from a child under 13, or (iii) the subject of the information in the case of information related to an individual that was collected online from another individual. The complainant must have made a good faith attempt to resolve her/his complaint directly with the organization or individual about which he or she is complaining, following the procedures set out in that organization's or individual's statement of its privacy policies.

2.3 ELIGIBLE CLAIMS

The complaint must allege that the organization or individual that collected the identifying information from the complainant online has:

a) used such information in a manner inconsistent with its published online privacy policies; or
b) in the case of a website displaying the BBB*OnLine* Privacy Program Seal, otherwise engaged in actions or practices with respect to the information collected from the individual online that are at variance with the BBB*OnLine* privacy guidelines applicable to that website.

The complaint must include information to support the complainant's allegation(s). In addition, the claim must not be ineligible for one of the reasons stated below.

2.4 INELIGIBLE CLAIMS

PPRS shall not consider a claim:

- in which the complainant is only seeking some form of monetary damages;
- in which the complainant is only alleging fraud or other violations of statutory or regulatory law;
- in which the respondent is a non seal participant that is participating in another seal program that provides for an adequate dispute resolution process including the provision of written decisions within a reasonable time after the process is initiated; or

- that has been resolved under a previous court action, arbitration or other form of dispute settlement.

Unless both parties agree, PPRS shall not consider a claim:

- that is currently in litigation or the subject of any other adjudicatory process (including claims submitted for resolution through binding arbitration); or
- as to which the complainant has previously agreed to use some other form of dispute resolution.

2.5 Available Remedies

A complainant may seek to have the information that she or he submitted online which is the subject of the complaint used in a manner consistent with the company's published privacy policies and, if applicable, the BBB*OnLine* Online Privacy Program guidelines. A complainant also may seek to have that information corrected.

PPRS or PRAB may require corrective action in the form of a change in online privacy policies or practices if, based on the evidence in the case, it deems such action to be required to avoid recurrences of the problem that is the subject of the complaint.

Neither PPRS nor PRAB can direct any corrective action that would require:

- monetary damages; or
- relief that would require the respondent to violate legal requirements imposed on it.

If the otherwise appropriate corrective action in a case would require the respondent to violate legal requirements, the respondent's continued eligibility to display the seal will be reviewed.

2.6 Intake Function

Intake is the first point of contact for those who wish to obtain information or make a complaint under the BBB*OnLine* Online Privacy Program Dispute Resolution Process. Upon receipt of any customer contact, the intake staff will record basic information from the individual and determine whether the contact is a general question or a potential complaint and will then handle the matter accordingly.

2.7 Handling Of General Inquiries

If the contact is a question or request for information, the intake staff will promptly answer the inquiry and, if appropriate, furnish informational materials to the inquirer and/or provide information as to the availability of online information that may be responsive to the question.

2.8 Handling Of Potential Complaints

2.8.1 Inquiry into status of potential respondent

When the intake staff believes the contact is a potential complaint, its first step will be to determine whether the potential respondent is a seal participant or not and, if it is not, whether it has an acceptable dispute resolution program. If it does have such a program, the individual will be referred to that program. If it does not, the intake staff will proceed with processing of the complaint.

2.8.2 Inquiry into prior attempt to resolve the complaint

After determining the status of the potential respondent, the intake staff will inquire into whether the complainant has made an attempt to resolve the complaint through contact with the organization or individual complained about. If the person submitting the complaint indicates there was, he/she will be asked to describe the contact and the results where such

information was not already provided and intake will proceed to the next step. If he/she indicates there was no attempt to resolve the complaint through contact with the organization or individual, he/she will be asked to try to so resolve the complaint and, in the case of a Privacy Seal participant, will be given information as to the person(s) to be contacted. The individual will be advised that he/she can return to the intake staff if his/her attempt to resolve the complaint does not yield satisfactory results.

2.8.3 Verifying identity of complainant and representative

After ascertaining that there has been a prior good faith attempt to resolve the issue with the organization or individual, the intake staff will undertake some inquiry into the identity of the person making the contact to attempt to verify to the extent possible that she/he is the person she/he is representing himself to be. If the person making the contact is doing so in a representative capacity, the staff also will undertake to verify that capacity as well as the person's identity.

2.8.4 Forwarding potential complaint to complaint review process

Whenever the intake center concludes it has adequate information about a prior attempt to resolve a potential complaint, it shall promptly provide the person submitting the complaint with an acknowledgement of its receipt of the complaint and forward the complaint for PPRS complaint review.

Part 3 DISPUTE RESOLUTION BY THE BBBONLINE PRIVACY POLICY REVIEW SERVICE (PPRS)

3.1 FUNCTION OF PPRS IN DISPUTE RESOLUTION PROCESS

PPRS shall be responsible in the dispute resolution process for determining the eligibility of a complaint and evaluating, investigating, analyzing, and making a decision on the merits of an eligible complaint.

3.2 INFORMATION IN PPRS PROCEEDINGS

3.2.1 Information required to sustain a complaint

Information submitted by the complainant should include a description of the respondent's disposition of the individual's initial complaint to it and must be sufficiently complete to permit the respondent and the PPRS staff to adequately evaluate the complaint. The PPRS staff shall be the sole judge of whether the information submitted is sufficiently complete to permit the opening of a case after providing the complainant with an opportunity to submit any additional information it deems necessary.

3.2.2 When information may be treated as confidential

A respondent or complainant may submit information to PPRS with the request that such information not be made available to the other party. A party seeking such treatment shall: (i) identify in its submission which materials are confidential and which are not; and (ii) affirm that the information for which confidentiality is claimed is not publicly available. Any information submitted with a request that it be held in confidence shall be returned to the submitting party or destroyed promptly upon conclusion of the PPRS proceedings.

3.2.3 Providing a nonconfidential summary of confidential information

Where a party submits material with a request that it be treated as confidential, the other party is entitled to receive a nonconfidential summary of such material that does not reveal any confidential matter but provides sufficient information about the material to allow the other party to respond to it. PPRS staff will assist a party in providing this summary where such assistance is desired. Failure of the respondent or complainant to provide an acceptable summary for this purpose will result in the information's not being considered in evaluation of the complaint. PPRS staff shall be the sole judge of the acceptability of a summary offered by either party

3.3 PPRS COMPLAINT REVIEW

Upon receipt of a potential complaint from the Intake Center, PPRS shall promptly determine whether the complainant has an eligible complaint and take one of the following actions.

- Whenever PPRS, in its sole judgment, concludes that the privacy complaint is an eligible complaint and contains all necessary information, PPRS shall docket the complaint as a case. It shall then promptly forward the complaint to the respondent for its answer with a summary of the confidential information, if any, submitted by the complainant.

- If PPRS, in its sole judgment, concludes that additional information is needed to sustain the complaint, it shall promptly contact the person who submitted the complaint and advise/her of the need for the further information for the process to go forward. If PPRS receives the requested information on a timely basis, it shall docket the complaint as a case and promptly forward the complaint to the respondent for its answer with a summary of the confidential information, if any, submitted by the complainant. If PPRS does not receive the requested information

within 10 business days of its request, it shall advise the person that submitted the complaint that it cannot proceed with investigation of the complaint and it shall discontinue any further action on the complaint.

- If PPRS, in its sole judgment, concludes that the complaint does not meet the PPRS eligibility guidelines for reasons other than a lack of information, it shall advise the complainant that it cannot proceed with investigation of the complaint and it shall discontinue any further action on the complaint. Where appropriate, PPRS shall provide the complainant with the name and address of any agency or group which may have jurisdiction over the complaint.

3.4 Replies And Responses To Complaint And Requests From PPRS

3.4.1 Respondent's answer to a complaint

After docketing a complaint as a case, PPRS shall forward the complaint to the respondent and request an answer. The respondent has 15 business days after receipt of the complaint to submit a substantial written answer, that is, an answer that includes some facts or information to support its responses to the complaint. If PPRS considers an answer to be deficient in this respect, it shall request a further answer by a time that it shall designate.

3.4.2 Complainant's reply to respondent's answer

When the respondent submits a substantial written answer, PPRS shall promptly forward that answer to the complainant, except for any material designated as confidential (see Section 4.2.2). The complainant has 10 business days after receipt of the answer to submit a written reply to the answer. If the complainant does not submit a reply, PPRS shall proceed to decide the case following the expiration of the complainant's time to reply, subject to a request by it for additional comments or data under section 4.4.4.

3.4.3 Respondent's response to a reply

If the complainant submits a reply, PPRS shall promptly forward that reply to the respondent. The respondent has 10 business days after receipt of the reply, to submit a written response. On receipt of the response or expiration of the time limit for submission of a response, PPRS shall proceed to decide the case, subject to a request by it for additional comments or data under section 4.4.4.

3.4.4 PPRS request for additional information or comments

In the event that PPRS requests comments or information from a respondent or complainant in addition to the answer, reply and response provided for above, the party receiving the request has six business days after receipt of the request to submit a written response thereto. On receipt of any such response, PPRS shall immediately forward it to the other party, who will have six business days after receipt to submit its response to the submission.

If a party fails to respond to the PPRS request for additional information or comments or fails to respond to the other party's submission in response to such request, PPRS shall proceed with its consideration of the case giving the fact of such nonresponse such weight as PPRS deems appropriate.

3.4.5 Conferences

PPRS, in its discretion, may accept a proposal by a respondent or complainant for a conference to be held within 10 business days after PPRS's receipt of the last written submission in the matter as an addition to the written submissions provided for under the preceding paragraphs, or may request such a conference on its own. A party's proposal or PPRS's request shall delineate the reasons for requesting such conference, a date, the identity of the participants in the conference, and the agenda. Where the conference is proposed by a party, the proposed date must have been agreed to by the other party if it wishes to

participate in the conference. The conference shall be held by teleconference or other electronic means and be limited to oral discussion of the matter without any written submissions.

3.4.6 Failure to answer a complaint

If a respondent fails to file a substantial written answer to the complaint within the period provided in 4.4.1 or fails to make a timely response to a PPRS request for a further answer, PPRS shall advise the respondent that its default will be noted in the next periodic report and that unless the respondent files a substantial written answer to the complaint within 15 days after receipt of this notice it will refer the matter to the appropriate government agency and, in the case of a seal participant, withdraw or suspend the seal.

If the respondent files a timely answer after this notice, the answer will be forwarded to the complainant as provided for in section 4.4.2 and the case will proceed from that point on in the manner prescribed in sections 4.4, 4.5 and 4.6.

If the respondent fails to file a timely answer after this notice, PPRS shall refer the file to the appropriate government agency and shall report the matter and the referral in the next periodic PPRS reports. In addition, if the respondent is a BBB*OnLine* privacy seal program participant, PPRS shall withdraw or suspend the seal.

3.4.7 Late filings

For a submission under this section to be timely, it must be received by PPRS within the specified period for submission. The parties may agree between themselves to extend the time limits specified in this section. In such case, the agreed upon limits will be controlling upon PPRS's receipt of a copy of the parties' agreement. If a party files a reply or response or submits requested information after the specified time limits, the untimely document shall not be considered by PPRS, unless the party receives an extension for good cause. No party shall receive more than one extension and no extension granted by PPRS shall exceed 20 business days, except in extraordinary circumstances.

3.5 PPRS Case Record

The case record in a PPRS proceeding shall include any answer, reply and responses submitted under the provisions of this part, except for any material submitted as part of such documents which has been designated as confidential. No submissions other than those provided for in this chapter shall be accepted as part of the case record, and any other submissions received by PPRS shall be returned promptly to the submitter when PPRS issues a decision or closes a case without a decision.

3.6 PPRS Decisions

3.6.1 PPRS's "Findings, Recommendations and Conclusions"

Where PPRS has docketed a complaint as a case and has not closed the case because of the respondent's nonparticipation, it shall formulate its judgment on the merits of the case in a statement of "findings, recommendations and conclusions" including any necessary corrective action and a time frame for such action. It shall complete this statement within 15 business days of its receipt of the last document authorized by section 4.4 or the expiration of the time limit for submitting such document. It shall then promptly provide a copy of such statement to the respondent and offer it an opportunity to submit, within 10 business days of its receipt of the document, a brief statement for inclusion in the final decision.

Where corrective action is required, PPRS shall request a statement within the 10 day period that includes a statement as to whether the respondent agrees to take the corrective action(s) or chooses to take the issues to appeal, under Part 5. The respondent's time to submit a statement may be extended for good cause. The statement shall not become public before issuance of a final decision.

3.6.2 Finalizing a decision where corrective action is not required

Where corrective action is not required, PPRS will proceed to issue a final decision promptly on receipt of the respondent's statement for inclusion in such decision or expiration of the time limit for such submission. The decision shall include the statement of "findings, recommendations and conclusions" and any statement submitted by the respondent in response thereto. A copy of such decision will be provided to the parties on issuance, and made available to the public. The decision will also be noted in the next periodic reports (see Part 7).

3.6.3 Finalizing a decision where corrective action is required

A final decision shall include the statement of "findings, recommendations and conclusions" and any statement submitted by the respondent in response thereto.

If, in a case where corrective action is required, the respondent submits a timely statement indicating an intention to take the required corrective action or to appeal, PPRS shall immediately issue its final decision and provide the respondent and the complainant with copies. The decision will also be made available to the public and noted in the next periodic reports (see Part 7).

If the required corrective action includes a direction to change online privacy policies or practices, and the respondent submits a timely statement asserting that the required action is impossible to perform, PPRS shall promptly consider such claim. To be considered, a statement claiming impossibility of performance must include a specific statement of the factors that give rise to the impossibility and contain facts to support the assertions. If PPRS finds that a statement is lacking in the necessary specificity, it shall promptly advise the respondent that it has 5 business days from receipt of the notification to submit a statement of its intention with regard to taking the corrective action or appealing. If PPRS finds the statement contains the required specificity, it shall proceed to evaluate the claim with such additional evidence as it deems necessary and issue a decision that either modifies its earlier findings, recommendations and conclusions or affirms them. It shall then forward this statement to the respondent, with a request for a statement of intent within 5 business days from receipt.

If the respondent does not provide a timely statement indicating an intent to take corrective action or appeal, PPRS shall issue its final decision and provide the respondent and complainant with copies. PPRS also shall refer the file to the appropriate government agency and shall report the respondent's nonparticipation and the referral as well as the decision in the next periodic PPRS reports. In addition, if the respondent is a BBB*OnLine* privacy seal program participant, PPRS shall withdraw or suspend the seal.

Part 4 Appeals TO PRAB

4.1 DISCRETIONARY APPEALS

Any seal participant or complainant complaining about a seal participant may appeal a PPRS decision adverse in whole or part to their position if PRAB determines that:

- seal participants, the public and/or BBB*OnLine* staff would benefit from a PRAB panel's resolution of a substantial and important question regarding the interpretation or applicability of BBB*OnLine* privacy standards applicable to the case; or
- there is a substantial possibility that a PRAB panel would decide the matter differently.

4.2 RIGHT TO APPEAL

A seal participant may appeal a PPRS final decision that includes corrective action requiring, either directly or as an indirect consequence of compliance with the decision, a significant change in the participant's company policies or practices applicable to all or a category of individuals from whom information is collected online.

4.3 FILINGS IN AN APPEAL

4.3.1 Filing an appeal

The complainant or respondent may seek an appeal under this part by submitting to PRAB, within 5 business days of receipt of the final case decision a letter requesting an appeal. The letter shall specify the issues the party wishes to appeal, state whether the appeal is sought as of right or on discretionary grounds, and explain how the appeal qualifies on such grounds. A copy of the letter shall be sent by the party initiating the appeal (the appellant), to the other party (the appellee). PRAB shall, in its sole judgment, decide whether the requested appeal is warranted and advise the parties of its decision.

4.3.2 Filing a cross appeal

If PRAB grants an appeal, the appellee shall have the right to appeal any additional issues considered by the PPRS that have not been appealed by the appellant To exercise this right, the appellee shall submit a letter of appeal to PRAB within 5 business days of receipt of the PRAB letter granting the appeal and copy the letter to the appellant. The letter shall specify the issues the appellee wishes to appeal.

4.3.3 Explanation of reasons for appeal

Any party appealing shall, within 10 business days of the receipt of the case record prepared by PPRS, submit to PRAB a letter explaining its position. It shall also forward a copy of its letter to the other party, who shall have 10 business days in which to submit a response to PRAB with a copy to the other party.

4.3.4 Late filings

If a party files an appeal or cross appeal or submits an explanation of the reasons for appeal after the specified time limits, the untimely document shall not be considered by PRAB, unless the party receives an extension for good cause. No party shall receive more than one extension and no extension granted by PRAB shall exceed 20 business days, except in extraordinary circumstances.

4.4 Forwarding of Case Record to the Parties

Whenever PRAB determines an appeal is warranted, it shall forward a copy of the appeal letter to PPRS within 2 business days of its decision, and forward any subsequent letter of cross appeal promptly on its receipt.

Within 5 business days after receipt of notification from PRAB of a letter requesting a cross appeal or, if later, the expiration of the time limit for receipt of such notification, PPRS shall prepare the relevant portions of the case record and forward them to PRAB. PRAB shall thereafter mail the case record to the parties.

4.5 Record on Appeal

The record on appeal shall consist of the case record portions furnished by PPRS, the PPRS decision, the letters of appeal and the submissions under section 5.3. No other written submissions shall be made during the appeal unless a) a party chooses to resubmit confidential information submitted below or is asked to do so by PRAB, or b) PPRS, on its own initiative or at the request of the panel, submits written information to the panel. Any participation by PPRS in PRAB proceedings is to represent the public interest in the integrity of the program.

4.6 Appointment of PRAB Chair And Members

4.6.1 Appointment of the Chair

The BBB*OnLine* Board shall select a person to serve as Chair of the PRAB.

4.6.2 Appointment of PRAB members

The BBB*OnLine* Board shall nominate persons to serve as "public", "data expert", and "company" members of the PRAB to be appointed by the PRAB Chair. These PRAB members will serve as the source of appointees for individual panels. Nominations shall be made whenever there is a need for additional members.

To qualify as a data expert member, an individual must have substantial technical experience in areas such as electronic data management, information systems, website management, etc. To qualify as a company member, an individual must be employed by a seal participant.

4.7 Appointment of Panel

4.7.1 Appointment by Chair

Upon granting of an appeal, the PRAB Chair shall proceed with appointment of a panel composed of PRAB members to hear the case, including designation of the panel member who will serve as its Chair. The Chair shall endeavor to appoint a panel that can hold a hearing within 20 business days of receipt of the last submission.

4.7.2 Eligibility of panelists

A company PRAB member will be considered as not qualified to sit on a particular panel if her/his employing company or corporate affiliate is the respondent, sells a product or service which directly competes with the product or service of the respondent involved in the proceeding or represents such an organization, or has any other conflict. A PRAB member, including a noncompany member, shall disqualify himself/herself from service on a panel if for any reason arising out of past or present employment or affiliation he/she believes that he/she cannot reach a completely unbiased decision. In addition,

PRAB shall inform the appellant and appellee of their right to object, for cause, to the inclusion of individual panel members, and to request that replacement members be appointed. Such requests will be subject to approval by the PRAB Chair.

4.7.3 Composition of panel

Each panel shall be composed of one "public" member, one " data expert" member, and one "company" member. The panel will meet at the call of its Chair, who will preside over its meetings, hearings and deliberations. The concurring vote of two of the three panel members is required to decide any substantive question before the panel. Any panel member may write a separate concurring or dissenting opinion which will be published with the majority opinion.

4.8 Procedure of Panel

As soon as the panel has been selected, PRAB will inform all parties as to the identity of the panel members. At the same time, staff will mail copies of the then record on appeal to each of the panel members, and will, in like manner, send them any subsequent response or request submitted by either party or PPRS under sections 5.3.3 or 5.5.

The panel, under the direction of its Chair, should proceed with informality and speed. All parties to a matter before the panel and PPRS shall be given 10 days notice of any hearing at which the matter is to be presented to the panel. Such notice shall set out the date and place of the hearing, and the procedure to be followed.

In the absence of the agreement of the parties, no facts or arguments will be considered by the panel if they are outside the facts in the PPRS Case Record or inconsistent with the arguments made before PPRS as reflected in that record. In the event a party offers newly discovered evidence germane to the issues before the panel which was not reasonably available to it during the PPRS proceedings, the panel may remand the case back to PPRS for its further consideration and decision.

The decision of the panel will be based upon the record on appeal and any summaries or arguments presented during the hearing. If a party has submitted confidential information on the appeal, the panel will honor the request for confidentiality, even though the party may have instituted the appeal, and will exclude the other party from the hearing during any discussion of the confidential material.

4.9 Panel Decisions

4.9.1 Issuance of a decision

The panel shall endeavor to forward its written decision, including the rationale for its conclusion to the PRAB Chair within 15 business days after the hearing. Upon receipt of a panel's decision, PRAB shall transmit such decision to the parties in the appeal. If the decision is in favor of the party who was the complainant in the PPRS proceedings, PRAB will ask the respondent to furnish it, within five business days of receipt of the decision, with a brief statement indicating its intentions with regard to implementing the corrective action directed by the decision and any comments it may wish to make on the decision. Except as provided in the following paragraph, on receipt of such statement, PRAB shall forward the statement and the decision to the other party, and make the decision public.

If the PRAB decision requires a change in online privacy policies or practices that was not required by the PPRS decision and the respondent's statement asserts that the required action is impossible to perform, PRAB shall promptly consider such claim. To be considered, a statement claiming impossibility of performance must include a specific statement of the factors that give rise to the impossibility and contain facts to support the assertions. If PRAB finds that a statement is lacking in the necessary specificity, it shall promptly advise the respondent that it has 5 business days from receipt of the notification to submit a statement of its intention with regard to taking the corrective action. If PRAB finds the statement contains the required specificity, it shall proceed to evaluate the claim with such additional evidence as it deems necessary and issue a decision that either modifies its earlier decision or affirms it. It shall then forward this decision to the parties with a request for a statement of intent from the respondent within 5 business days from receipt.

4.9.2 Noncompliance with a decision

If the decision is in favor of the complainant and the respondent fails to indicate within the five day period described in section 5.9.1 that it intends to take the required corrective action(s), the Chair shall issue a Notice of Intent to the respondent. The Notice shall advise the respondent that the case will be referred to the appropriate government agency, and seal compliance review will be undertaken, within 10 business days of the respondent's receipt of the Notice, unless the Chair is notified by that date of the respondent's intent to take the corrective action. If the respondent does not submit a timely response indicating an intent to take the corrective action, the Chair shall direct that the matter be referred and that PPRS be notified of the need to withdraw or suspend the seal. PRAB shall also forward the decision to the other party and make the decision public, and the respondent's noncompliance and the referral shall be noted in the next periodic reports.

Part 5 Closing a case

A dispute resolution file on a case shall be closed when:

1. PPRS has issued a final decision and neither party has requested an appeal within the time limits or a requested appeal has not been granted;
2. PRAB has issued a decision in favor of the respondent or the respondent has agreed to comply with a PRAB decision in favor of the complainant;
3. PPRS or PRAB has referred the matter to a government agency because of the respondent's nonparticipation in the process or failure to comply with a decision; or
4. PPRS or PRAB refuses to proceed with the case because of a party's failure to abide by its agreement under section 1.5 to hold information in confidence.

When a case has been closed, no further materially similar complaints on the claim(s) in question need be accepted by PPRS and where closure results from a decision on the merits, no further materially similar complaint on the claim(s) in question shall be accepted by PPRS.

Part 6 Reporting Of PPRS/PRAB Activity And Publication Of Decisions

PPRS shall publish PPRS reports at least 4 times each year, summarizing matters concluded during the previous period. These reports shall:

With respect to public inquiries, provide a statistical summary of the number and nature of contacts from the public and the actions taken by the PPRS with respect to those inquiries.

With respect to complaints:

Provide a statistical report of the number and nature of complaints deemed ineligible for processing during the period, including the specific reason for a determination of ineligibility;

Provide a statistical report of the number of cases decided during the period, including the number decided in the complainant's favor and the number in the respondent's favor and the type of corrective action required (correction of error that occurred in individual case, change in policy, change in practice).

For each complaint deemed eligible in which a respondent organization or individual fails to submit a timely answer and/or declines to participate in the PPRS process, provide a summary report (including the name of the organization) of the nature of the claim and the PPRS action in the case.

PPRS decisions and PRAB decisions shall be published on the BBB*OnLine* website promptly after issuance.

APPENDIX C

BBB*OnLine*® Privacy Program Dispute Resolution Process

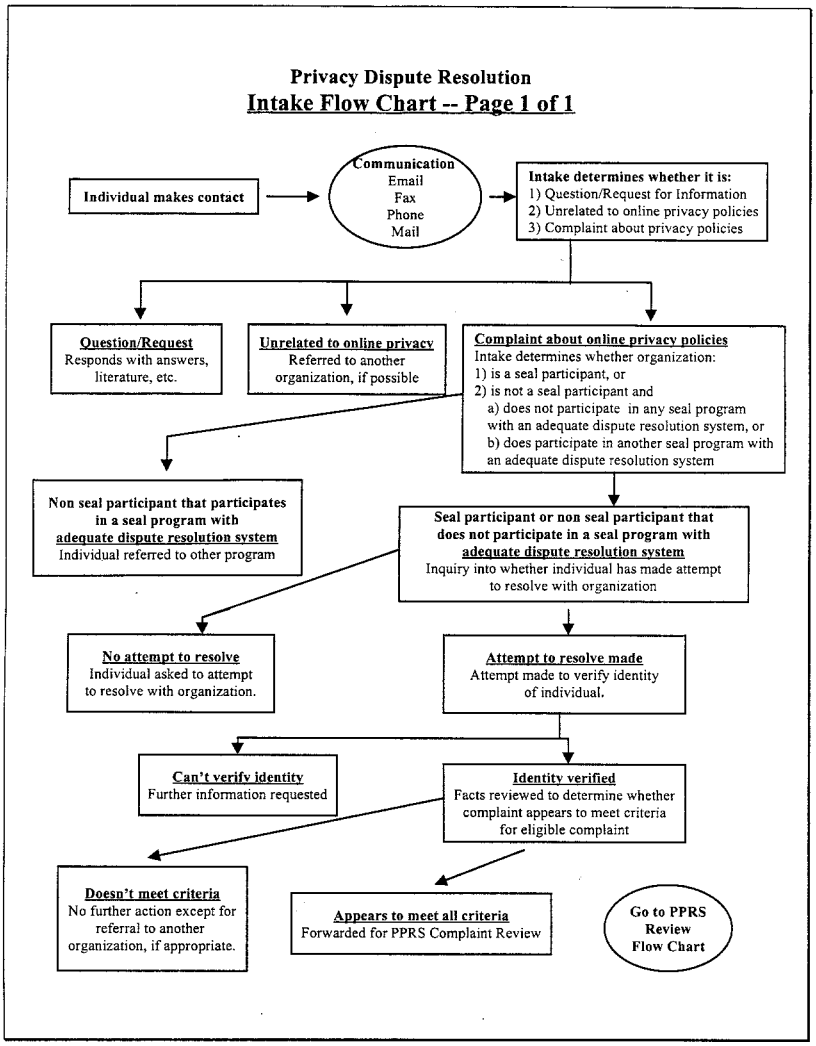
Intake

PPRS

PRAB

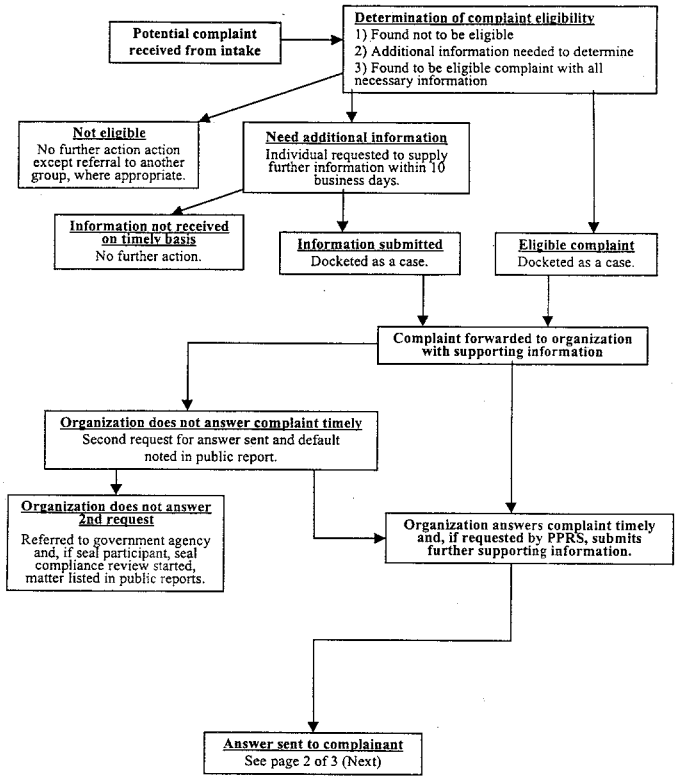
Flow Charts

Copyright © 1999 Council of Better Business Bureaus, Inc.


Privacy Dispute Resolution
Intake Flow Chart -- Page 1 of 1
Individual makes contact
Communication
Email
Fax
Phone
Mail
Intake determines whether it is:
1) Question/Request for Information
2) Unrelated to online privacy policies
3) Complaint about privacy policies
Question/Request
Responds with answers, literature, etc.
Unrelated to online privacy
Referred to another organization, if possible
Complaint about online privacy policies
Intake determines whether organization:
1) is a seal participant, or
2) is not a seal participant and
a) does not participate in any seal program with an adequate dispute resolution system, or
b) does participate in another seal program with an adequate dispute resolution system
Non seal participant that participates in a seal program with adequate dispute resolution system
Individual referred to other program
Seal participant or non seal participant that does not participate in a seal program with adequate dispute resolution system
Inquiry into whether individual has made attempt to resolve with organization
No attempt to resolve
Individual asked to attempt to resolve with organization.
Attempt to resolve made
Attempt made to verify identity of individual.
Can't verify identity
Further information requested
Identity verified
Facts reviewed to determine whether complaint appears to meet criteria for eligible complaint
Doesn't meet criteria
No further action except for referral to another organization, if appropriate.
Appears to meet all criteria
Forwarded for PPRS Complaint Review
Go to PPRS Review Flow Chart

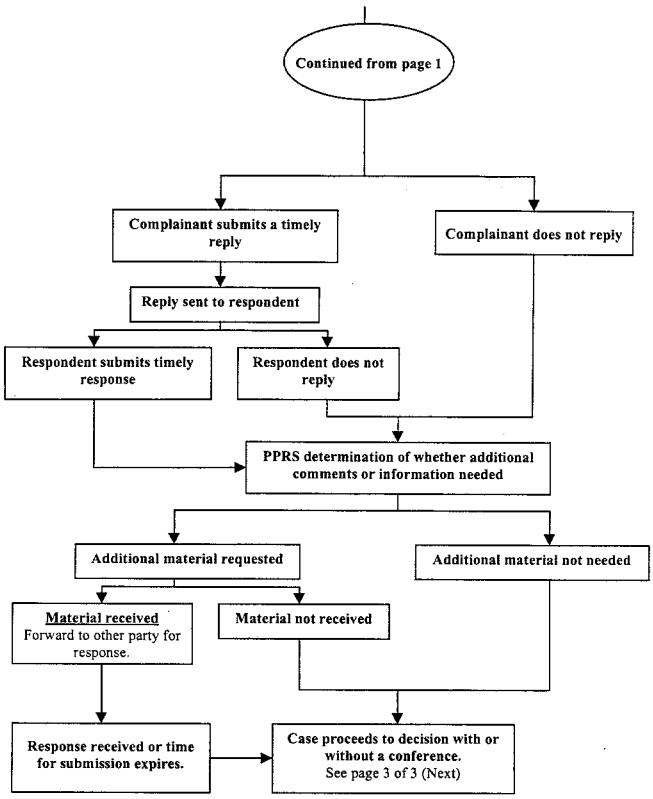
Privacy Dispute Resolution

PPRS Complaint Handling Flow Chart – Page 1 of 3



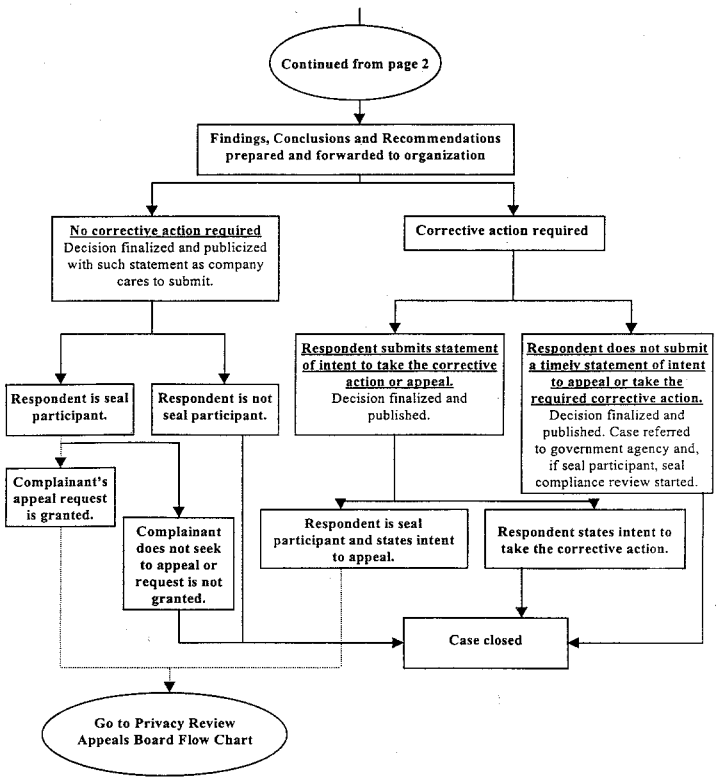
Privacy Dispute Resolution

PPRS Complaint Handling Flow Chart -- Page 2 of 3



Privacy Dispute Resolution

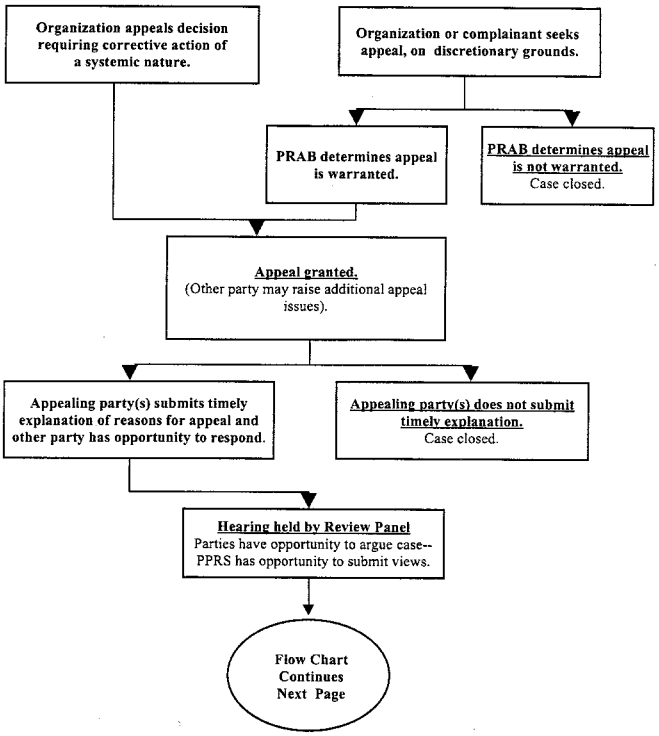
PPRS Complaint Handling Flow Chart -- Page 3 of 3



Privacy Dispute Resolution

Privacy Review Appeals Board Flow Chart -- Page 1 of 2

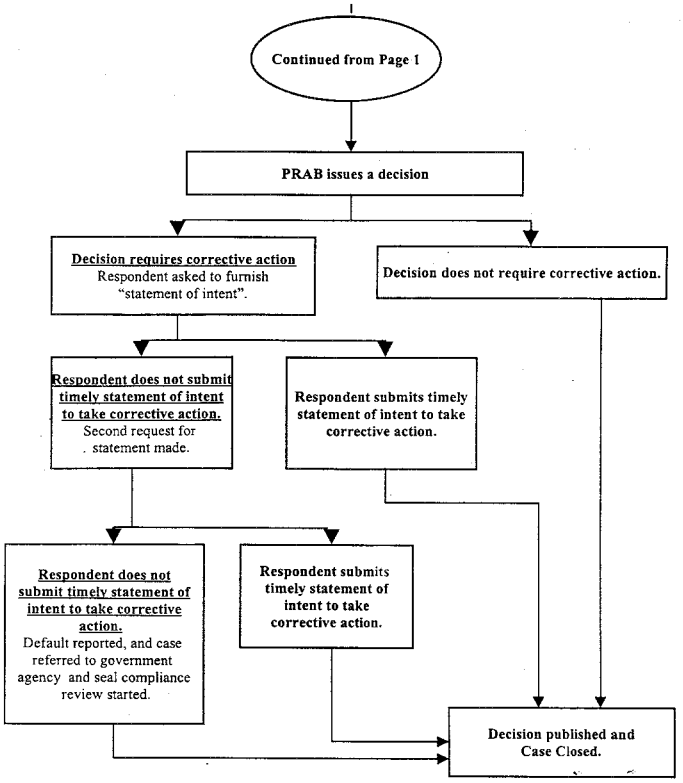
(Appeal process available only if organization is a seal participant)



Privacy Dispute Resolution

Privacy Review Appeals Board Flow Chart -- Page 2 of 2

(Appeal process available only if company is a seal participant)



BBB*OnLine*®
Online Privacy Dispute Resolution Process For Seal Program Participants

Intake

PPRS

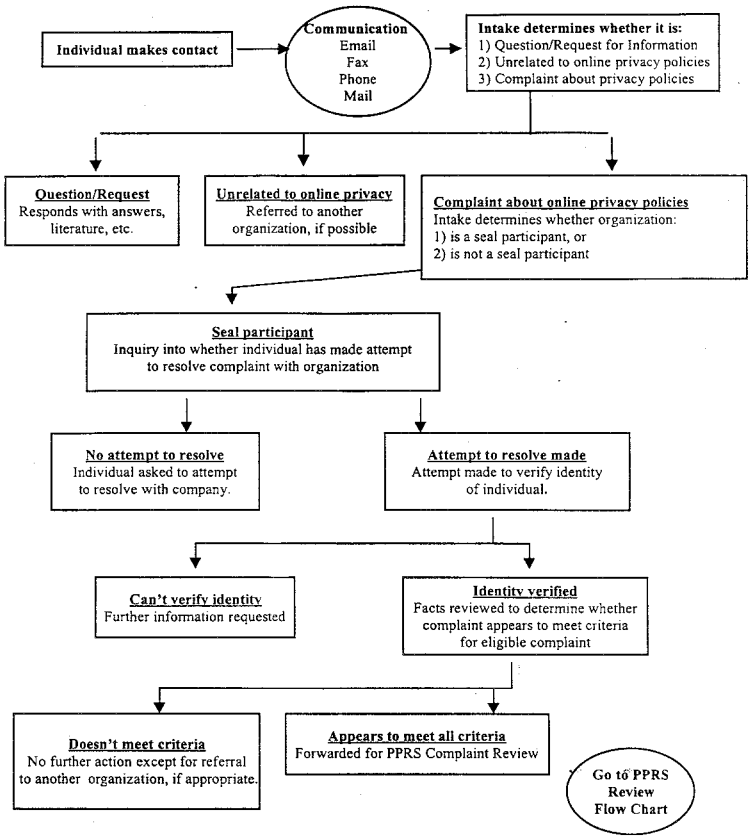
PRAB

Flow Charts

Copyright © 1999 Council of Better Business Bureaus, Inc.

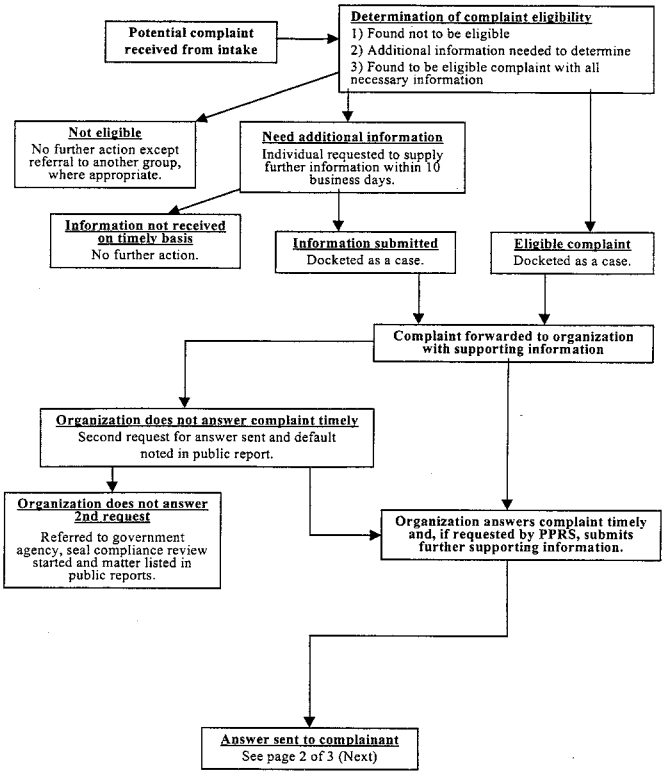
Privacy Dispute Resolution

Intake Flow Chart -- Seal Participants -- Page 1 of 1



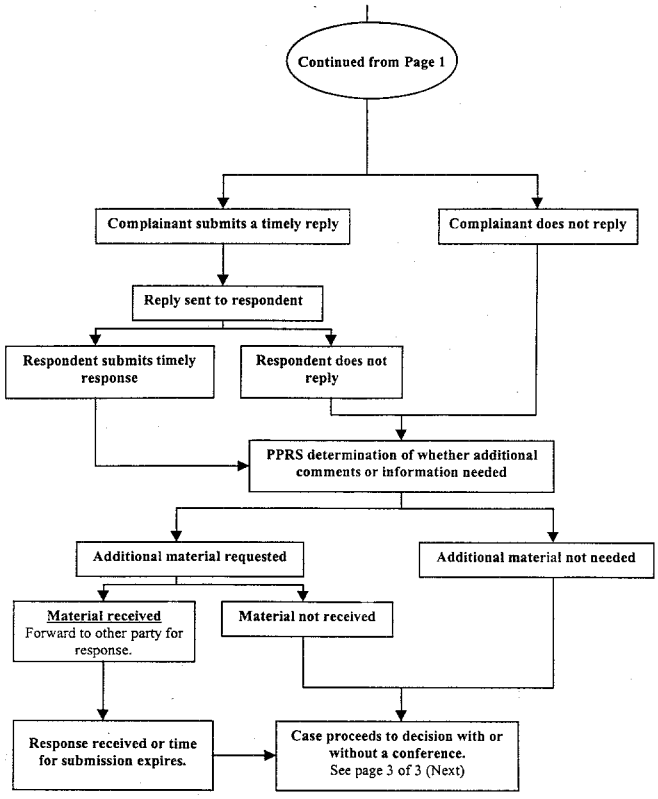
Privacy Dispute Resolution

PPRS Complaint Handling Flow Chart -- Seal Participant -- Page 1 of 3



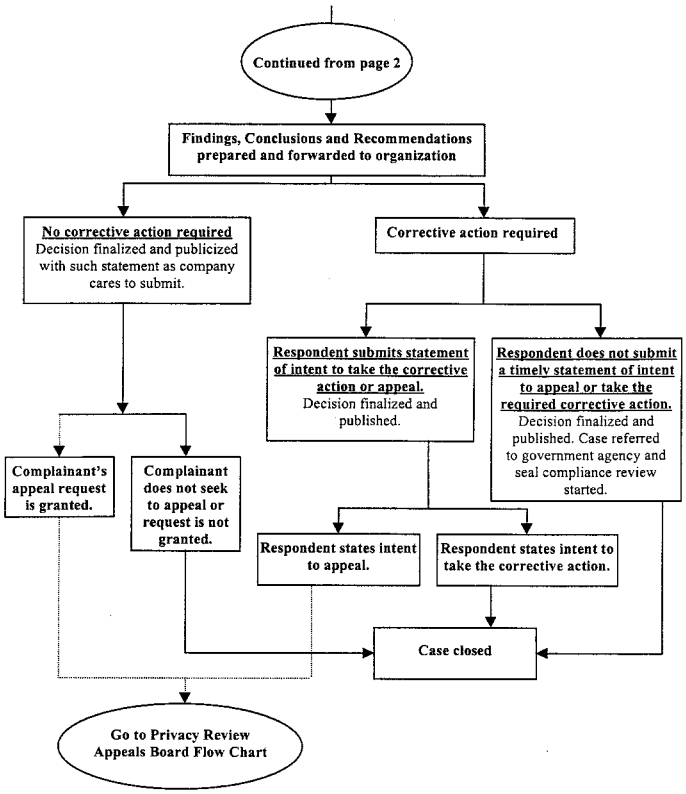
Privacy Dispute Resolution

PPRS Complaint Handling Flow Chart --Seal Participant -- Page 2 of 3



Privacy Dispute Resolution

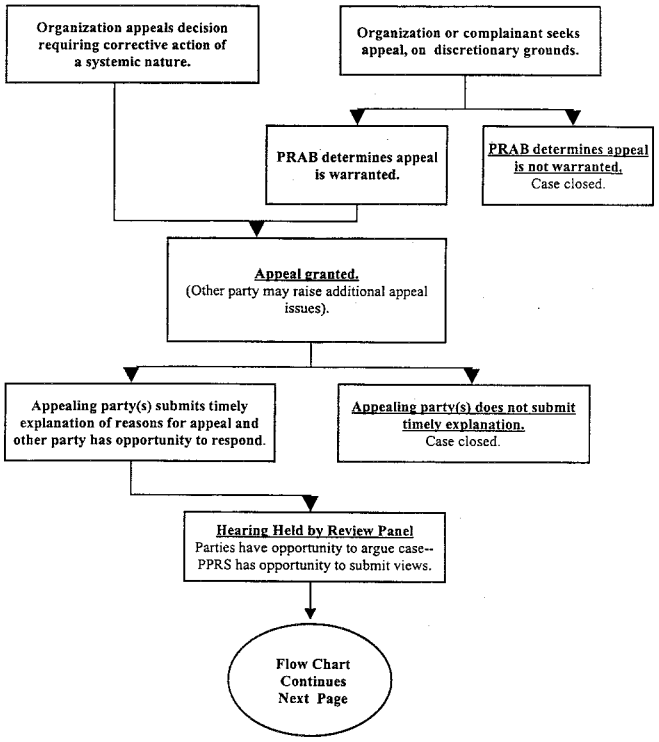
PPRS Complaint Handling Flow Chart -- Seal Participant -- Page 3 of 3



Privacy Dispute Resolution

Privacy Review Appeals Board Flow Chart -- Page 1 of 2

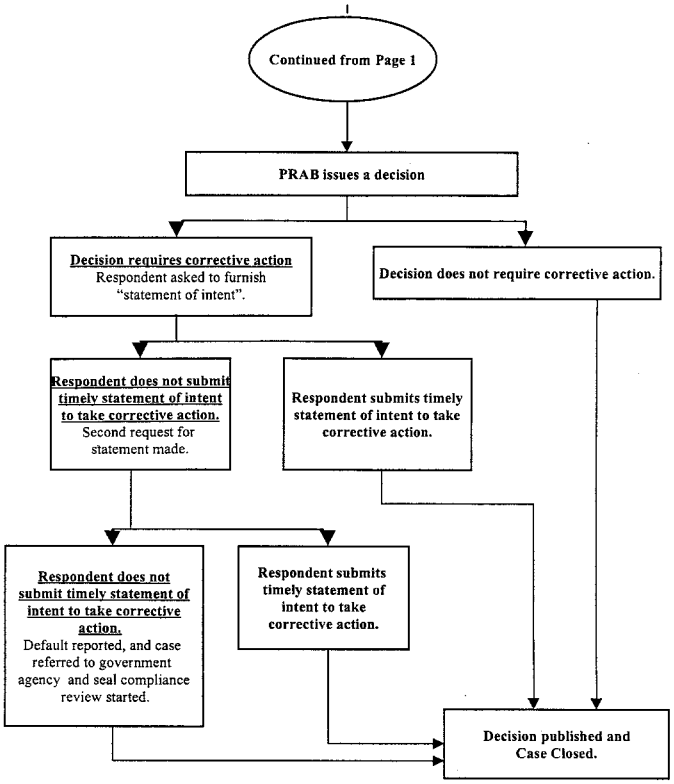
(Appeal process available only if organization is a seal participant)



Privacy Dispute Resolution

Privacy Review Appeals Board Flow Chart -- Page 2 of 2

(Appeal process available only if company is a seal participant)



BBB*OnLine*®
Online Privacy Dispute Resolution Process For Organizations Not Participating In Seal Program

Intake

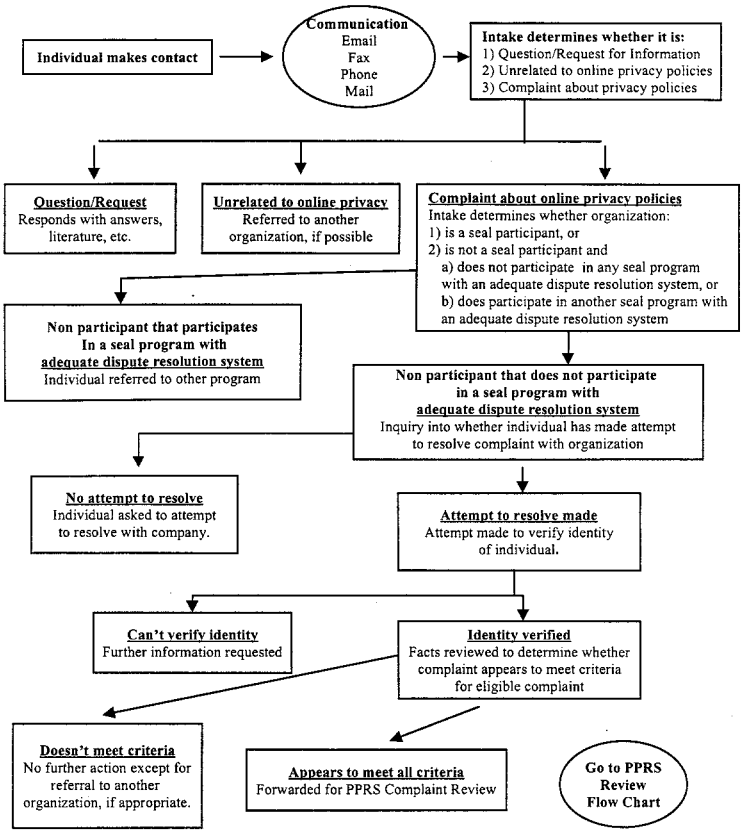
PPRS

Flow Charts

Copyright © 1999 Council of Better Business Bureaus, Inc.

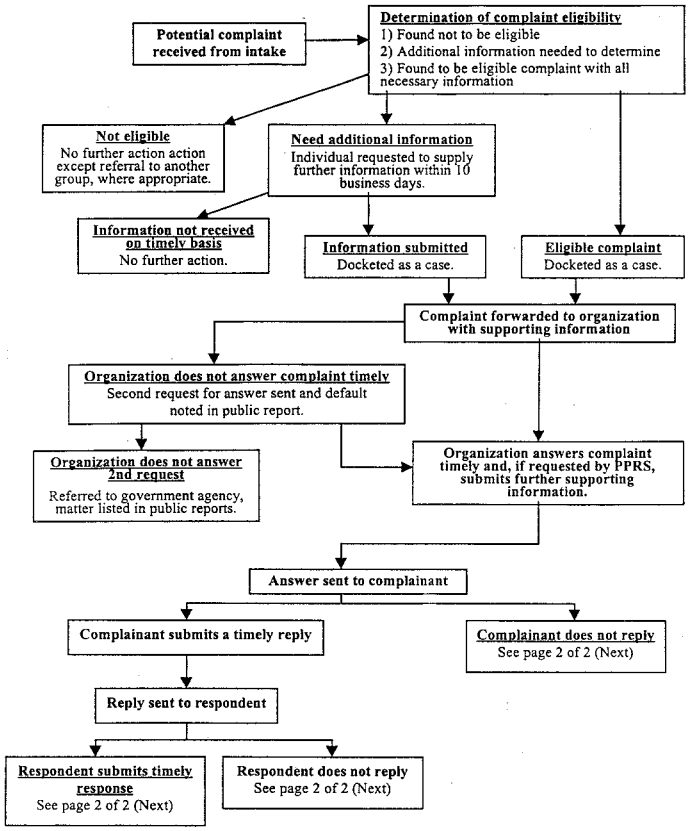
Privacy Dispute Resolution

Intake Flow Chart -- Non Seal Participants -- Page 1 of 1



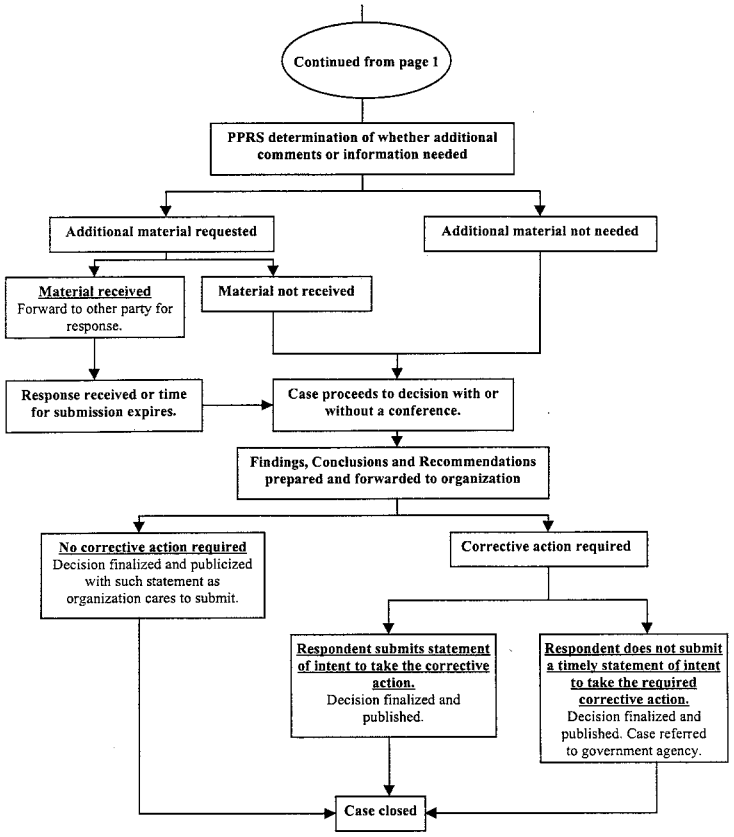
Privacy Dispute Resolution

PPRS Complaint Handling Flow Chart – Non Seal Participants – Page 1 of 2



Privacy Dispute Resolution

PPRS Complaint Handling Flow Chart – Non Seal Participants – Page 2 of 2



APPENDIX D

BBB*OnLine*® Privacy Program
Seal Price Schedule

Application Fee

All applicants pay a one-time non-refundable $75 processing fee.

Annual Seal Fee

Company Sales	Annual Participation Fee
$1 million or less	$150
$1,000,001 - $5,000,000	$300
$5,000,001 - $10,000,000	$450
$10,000,001 - $50,000,000	$750
$50,000,001 - $100,000,000	$1,000
$100,000,001 - $500,000,000	$1,500
$500,000,001 - $2,000,000,000	$2,000
Over $2 billion	$3,000

Appendix E

BBB*OnLine*® Privacy Program
Sample Media Coverage

"BBB to Help Guard Privacy On Internet" - *San Jose Mercury News*, March 17, 1999

"Progress Made In Online Data Privacy Talks" – *Financial Times*, March 19, 1999

"Better Business Bureaus Offer Online Privacy Seal" – *Washington Post*, March 17, 1999

"Council of Better Business Bureaus, Inc." – *Wall Street Journal*, March 18, 1999

"Business Group Unveils Plan for Online Privacy" – *New York Times*, March 18, 1999

"Seal of Online Privacy" – *Christian Science Monitor*, March 22, 1999

"Better Business Bureau to Start Online Privacy Seal Program" – *Bloomberg*, March 16, 1999

"Better Business Bureau Unit Starts Online-Privacy Seal Program" – *Bloomberg*, March 17, 1999

"BBB Web Site Privacy Program Finally Arrives" – *CNET News.com*, March 16, 1999

"Better Business Bureau Gets Personal" – *Interactive Week*, March 17, 1999

"Better Business Bureau Online? Maybe" – *Computerworld*, March 22, 1999

"Web Seal of Approval Ready" – *Privacy Journal*, April, 1999

San Jose Mercury News
March 17, 1999

BBB to help guard privacy on Internet

BY STEPHEN BUEL
Mercury News Staff Writer

The nation's best-known service for resolving disputes between consumers and businesses is joining the movement to police privacy online, a move that could help head off European sanctions against U.S. companies.

BBBOnline, the Internet arm of the 86-year-old Better Business Bureau, is launching a privacy seal designed to help consumers easily identify Web sites and online merchants that safeguard their credit, medical and other personal records.

Online privacy protection is emerging as a major consumer issue following December's record volume of online gift buying. As computer users flock to the Web, more Internet publishers and merchants are asking them to leave personal information behind.

Consequently, U.S. Internet firms are being urged to toughen their privacy

See **BBBONLINE**, *Page 13A*

INFORMATION FOR LIFE

BBB's Internet arm will help protect privacy

■ BBBONLINE

from Page 1A

safeguards. Federal officials have repeatedly warned the industry to get its house in order or risk federal regulation. U.S. negotiators also face a June 21 deadline for agreement with the European Union on standards for protecting personal data.

U.S. and EU negotiators met again Tuesday in an ongoing effort to develop standards that will satisfy much higher European expectations regarding the collection and use of personal data. Failure to resolve the issue will expose U.S. companies to a new European law prohibiting the transmission of such data to any country that fails to devise an acceptable standard — sanctions that could be devastating to U.S. Internet firms.

U.S. Undersecretary for International Trade David Aaron, who was briefed by the non-profit Better Business Bureau as it developed its new program, said the new safeguards could help persuade European Union officials to put their faith in the industry-led approach favored by the United States.

The program will include on-site inspections of member companies and a dispute-resolution process that will respond to consumer privacy complaints about participating — and even non-participating — Web sites, bureau officials said.

"The dispute settlement and the monitoring is a big part of what they like about it," Aaron, the chief U.S. negotiator, said of the program. But resistance to self-regulation remains strong in some countries, he added. "They tend to view industry self-governance as the fox guarding the chicken coop."

But European officials are likely to look with favor upon another aspect of the program — the requirement that consumers be able to gain access to all the information a member Web site collects on them. Firms won't be able to set unreasonable fees or conditions for providing this information, bureau general counsel Steve Cole said.

"For example, they can't charge you $15," Cole said. "They can't say, 'You can only come once every five years.' "

In many ways, the bureau's program resembles an existing one from Truste, a Palo Alto non-profit agency whose online privacy seals are displayed by about 500 major Web sites. But a bureau spokeswoman said the visibility of the bureau's brand name, coupled with the rigor of its approach, represents a major step forward for online privacy.

The bureau's program, which spokeswoman Sydney Rubin said about 350 companies have sought to join so far, will permit members to display one of two logos designed to let consumers know that the Web site they're visiting follows acceptable practices. The program will cost members an annual fee of between $150 and $3,000, depending on the company's sales volume.

Cole said the program will give consumers a mechanism for complaining about the use of personal data. After a complaint is filed electronically or by mail, Cole said, the bureau would forward a copy to the company in question and then attempt to resolve the issue and determine whether the company is living up to the program's standards.

"It's very important, as we see it, not just to post a privacy policy," Cole said. "The real issue is, 'Are you going to comply with it?' "

Although the bureau's program will lack financial penalties, Cole said he believed that few businesses would be willing to risk the bad publicity associated with having the bureau's privacy endorsement publicly withdrawn from their site.

But if that isn't a sufficient incentive to encourage businesses to comply with the bureau's policies, Cole said his agency will refer problem cases to the Federal Trade Commission, which has been known to take bureau referrals to court.

Companies wishing to join the program, or consumers wishing to file a complaint with a Web site, can obtain information at **www.bbbonline.org**

Financial Times
March 19, 1999

SELF-REGULATORY REGIMES US GROUPS CREATE WEB SITES DISPLAYING SEALS OF APPROVAL IF EU RULES ARE SATISFIED

Progress made in online data privacy talks

By Louise Kehoe in San Francisco and Nancy Dunne in Washington

US and EU negotiators say they have made "substantial progress" in this week's talks in Washington to head off another debilitating trans-Atlantic trade dispute, in this case over online data privacy.

With the US poised to impose duties on EU goods in retaliation for its banana import regime and with another row looming over hormone-treated beef, the two sides are working hard to make US self-regulatory regimes acceptable under the EU privacy directive.

The two sides will meet again in April with the hope of reaching a deal for the next US-EU summit in June.

In an effort to meet EU requirements, companies and US private sector groups are creating web sites which display seals of approval if their consumer data protection satisfies EU rules. The most rigorous programme was launched this week by Council of Better Business Bureaus (BBB), a US private sector organization that certifies the ethical standards of its members and mediates in disputes between consumers and businesses.

The "BBB online privacy seal" and a companion programme aimed at web sites designed to attract children examine every aspect of how internet merchants collect, store and protect consumers' personal data. The scheme goes beyond earlier efforts encouraging online businesses to disclose privacy policies and, in some cases, monitoring compliance.

Companies applying for the BBB seal must complete 140 questions covering issues as wide ranging as employee training on data privacy, computer security measures and third party access to data by business partners such as shipping companies or advertising agencies.

Some 350 online merchants have already begun the application process. One of the first companies to be granted the BBB privacy seal is expected to be Dell Computer, the leading online seller of personal computers.

As well as satisfying the BBB's criteria for approval, online businesses must submit to monitoring and review of their business practices and agree to co-operate with dispute resolution procedures. In a mov that could go a long wa toward satisfying EU demands, the BBB pro gramme also include enforcement mechanisms.

Russell Bodoff, chief oper ating officer of the BBB' new Online subsidiary, sai the organisation would pub lish the names of companie that failed to live up to thei promises and refer these cases to US authorities.

Washington Post
March 17, 1999

Better Business Bureaus Offer Online Privacy Seal

By ROBERT O'HARROW JR.
Washington Post Staff Writer

A subsidiary of the Council of Better Business Bureaus plans to begin a new effort to protect privacy on the Internet today, offering qualified companies an electronic seal verifying their commitment to use personal information properly.

BBBOnLine has been working on the seal program since early last summer, after calls from the Clinton administration for independent oversight of voluntary privacy policies online. Administration officials have said repeatedly that such enforcement is crucial for self-regulation to succeed.

Under the program, companies displaying the seal will have to spell out how they gather and use names, addresses and other personal information. They must give consumers a way to verify the accuracy of their data and be willing to work with officials at the BBBOnLine to resolve complaints. Companies that fail to follow through will lose the right to display the seal.

During a closed demonstration of the system at the Federal Trade Commission yesterday, BBBOnLine officials said they will take complaints from anyone and may refer some to the FTC, according to a person who attended the event and asked not to be named. About 350 companies have begun the process of filling out a detailed assessment form of their privacy policies, and BBBOnLine officials hope to have 1,500 enrolled by the end of the year, said the person, who was involved in the development of the program.

Fees for the seals will be as low as $150 and possibly as high as $3,000 for some companies. Dell Computer Corp. plans to display the seal on its Web site this morning.

Although development of the initiative took months longer than expected, BBBOnLine officials were optimistic the version set to go into operation today will satisfy consumer demands for privacy protections, while allowing commerce on the Internet to flourish.

In a letter announcing the

See PRIVACY, *E10, Col. 4*

Web Sites to Display Council's Privacy Seal

PRIVACY, *From E1*

launch, BBBOnLine President James L. Bast said, "We are very proud of this new initiative, and are especially gratified by the support we have received from business and government leaders over the past few months of its fast-track development."

Vice President Gore, who intends to make consumer privacy and the development of online commerce key issues in his presidential campaign, praised the program. "Privacy is a cherished American value, and I welcome efforts by the private sector to offer meaningful and enforceable privacy protections."

So did an official at TRUSTe, a nonprofit group that already offers its own privacy seal at several hundred Web sites. "We definitely need help out there," said TRUSTe Executive Director Susan Scott.

Privacy activists said it remains to be seen if either seal program will adequately hold companies accountable for how they use customers' personal information. Deirdre Mulligan, staff counsel at the Center for Democracy and Technology, said BBBOnLine has the potential for bringing far more attention to the issue because the Better Business Bureau is so widely known by businesses and consumers alike.

"This will help put privacy closer to the front of the queue," said Mulligan.

Wall Street Journal
March 18, 1999

COUNCIL OF BETTER BUSINESS BUREAUS INC.

BBBOnLine, a division of the Council of Better Business Bureaus Inc., based in Arlington, Va., unveiled its long-awaited Internet-privacy seal. The seal, which depicts a combination lock, will be posted on Web sites that participate in BBBOnline's privacy program. To earn the seal, Web sites must post a privacy policy telling users what personal information is being collected about them and how that information will be used. BBBOnLine will monitor sites' compliance with the posted policies, and will provide consumers with a forum to air and resolve privacy-related complaints.

March 18, 1999

Business Group Unveils Plan for Online Privacy

By JERI CLAUSING

WASHINGTON -- The Better Business Bureau on Wednesday launched its new program for certifying and monitoring the collection of personal data online, a long-awaited self-regulatory effort that businesses hope will help appease concerns by the European Union, the Federal Trade Commission and lawmakers that American companies have failed to offer adequate consumer protections in cyberspace.

The program, called BBBOnLine, gives qualified companies an electronic seal for their Web site verifying that they adhere to their stated practices about what information they collect from consumers and how it is used. It also requires them to submit to a dispute-resolution process when a customer complains and establishes a system of random audits for insuring that program participants remain in compliance.

Related Article
Professor Joins Administration to Work on Privacy Issues
(March 5, 1999)

Forum
Join a Discussion on Online Privacy

The program has been a year in the making. And its launch, several months later than anticipated, comes at a crucial time for the Clinton Administration, which has resisted calls to enact new laws for protecting the privacy of consumers in cyberspace. The Administration has staunchly advocated a laissez-faire approach despite a tough new European Union privacy directive that threatens to disrupt electronic commerce between the United States and Europe.

A key provision of that directive prohibits any company doing business in the European Union from transmitting personal data to any country that does not guarantee comparable privacy protections.

The Better Business Bureau on Tuesday evening reviewed its new program for the European Union's John Mogg, a director general, who was in town for negotiations with David Aaron, the Under Secretary of International Trade in the Commerce Department. The two are discussing what type of self-regulatory model would be acceptable for certification by the European Union's member states.

Although both Mogg and Aaron said they had made significant progress

and were encouraged by the program, they said they still had not reached agreement on two key areas: the amount of access customers should have to the data companies have collected about them, and mechanisms for enforcing privacy protections.

"We're making great progress," Aaron said. "The work is not finished, but we think it's going well."

He and Mogg plan to meet again the week after Easter, at which time they hope to finalize language for a draft agreement that could be submitted to the Administration and the EU for endorsement. The EU directive took effect last October, but the European Commission, the union's executive leadership, delayed sanctions against the United States for non-compliance until June 21 in hopes an agreement could be reached on an acceptable plan of self-regulation.

Although Mogg said he did not anticipate that this week's resignation of the entire European Commission, which has been accused of corruption, would affect that deadline, some privacy advocates said it could make Aaron's job of selling self-regulation tougher.

"That is significant because the member states have been pushing the commission to go further on privacy," said Marc Rotenberg, executive director of the Electronic Privacy Information Center, which has been seeking legislation to protect consumers against the resale and misuse of personal information collected electronically. "In other words, they have been more critical than the commission" of the U.S. policy against regulating companies in this area.

Rotenberg was also skeptical of the Better Business Bureau's seal program.

"I'm sort of the attitude right now that it's too little, too late," he said.

Others were less critical, but still reserved judgment.

"I think it is significant that the Federal Trade Commission and the BBB have both decided that these are critical consumer protection issues," said Deirdre Mulligan of the Center for Democracy and Technology. "I think that the BBB is saying to its members that privacy is something that we think is important... It sends a signal to the business community that privacy is something that they have to attend to."

The Federal Trade Commission, which after the threat of legislation last summer effectively pressured companies into an alliance that created the basis of the BBB plan, was also given a preview by the business bureau on Tuesday.

Vicki Streitfeld, a spokeswoman for the agency, said the program represents "good progress," but that a final judgment on whether self-regulation is working won't be made by the FTC until late this spring or early summer, when it expects to issue a new report to Congress.

In addition to monitoring how BBBOnLine is carried out and how many companies sign on, the FTC is awaiting results of an industry survey of

Related Article
FTC Report on Online Privacy Draws Quick Criticism

privacy practices by Web sites. The survey is a follow-up to one conducted by the agency last year, which found that few Web sites had privacy practices clearly posted and that numerous sites aimed children were collecting personal information.

Criticism (June 4, 1998)

Characterizing the results of that survey as dismal, the FTC won Congressional approval of legislation to mandate that Web sites get parental permission before collecting any personally identifiable information from children under 13. At the same time, it vowed to seek a new law extending those protections to adults if significant progress in self-regulation and self-enforcement were not made by early this year.

In promoting its new program at a Wednesday morning news conference, the Better Business Bureau emphasized its more than 80 years of experience in resolving disputes between consumers and businesses. It also said that it has signed up 2,600 online businesses for a similar but separate program that certifies Internet merchants as reliable businesses.

Although just one company, Dell Computer Corp., displayed the BBB seal on Wednesday, Russell Bodoff, senior vice president and chief operating officer of BBBOnLine, said more than 300 other companies had already initiated the application process, which has just opened.

"We expect our program to grow quickly," he said.

There are two separate seal programs, one indicating companies adhere to strict guidelines to protect children, the other for adults.

Companies can go through the entire certification and application process online. Companies do not have to be Better Business Bureau members, and application fees vary with the size of the company, starting at $150.

"We want this to be an open process," Bodoff said. "We want the only reason that a company can't participate to be because they can't meet our standards."

The seal program is not the first such attempt at certifying sites in cyberspace, but is the most comprehensive, offering random audits of compliance, mandatory dispute resolution and published decisions of all decisions against companies. BBBOnline said it also would work closely with the FTC, referring any cases its finds of deceptive or other illegal practices.

Related Sites

These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability.

- Better Business Bureau
- European Union
- Federal Trade Commission
- BBBOnLine
- Department of Commerce's International Trade Administration

Christian Science Monitor
March 22, 1999

Seal of online privacy

Sometimes, the Internet seems like an endless questionnaire. One Web site wants to know your birth date and income. Another won't let you log in until you type in your mother's maiden name.

The best sites promise up-front not to give out such personal data without your permission.

But is that what they actually do?

Last week the Better Business Bureau launched a new BBBOnline privacy seal aimed at answering just that. Although the privacy policies themselves vary, the seal certifies that companies treat personal data the way they say they do. As a minimum, online companies have an opt-out clause for people who don't want their information sold to other marketers.

BBBOnLine

"Businesses are starting to recognize that this is a high-level consumer concern," says Russ Bodoff, chief operating officer of BBBOnline (www.bbbonline.com).

To make sure a Web site won't sell your mother's maiden name to the highest bidder, check out its privacy policy. If it has the Better Business Bureau seal, so much the better. If it doesn't post a privacy policy at all, surf on by.

Mom will thank you.

Bloomberg
March 16, 1999

Better Business Bureau to Start Online-Privacy Seal Program

Washington, March 16 (Bloomberg) -- The Council of Better Business Bureaus' online subsidiary plans to start a long-awaited privacy program tomorrow in another bid by industry to fend off laws designed to protect U.S. consumers' privacy on the Internet.

BBBOnLine, sponsored by Microsoft Corp., AT&T Corp., International Business Machines Corp. and other companies, will use a seal program to let consumers know that a Web site adheres to certain privacy guidelines.

Lawmakers and regulators have said that if Internet companies don't improve privacy protections, Congress could pass legislation to curb how online personal data is collected and used.

The Better Business Bureau represents ``an established brand that has some consumer awareness and trust," said Bill Whyman, an Internet analyst with Legg Mason Inc.'s Precursor Group. ``This is about getting Mom and Pop consumers confident about the Internet."

Officials with the program scheduled a briefing in Washington, D.C. tomorrow. BBBOnLine officials said in November that the program, first announced in May, wouldn't be up and running until the first half of this year.

The Commerce Department estimates retail sales on the Internet will increase to $30 billion a year by 2000, though U.S. officials warn that growth could be stifled by consumers' concerns over privacy and security.

Web sites that display the BBBOnLine seal will be required to tell consumers what personal information is being collected and how it will be used. The program also will respond to consumer complaints and crack down on violations.

Another privacy-seal program, Truste, began in June 1997 and has signed up more than 500 Web sites, said Susan Scott, executive director of the industry-sponsored program. BBBOnLine ``will help amplify the issue in the industry," she said.

The Federal Trade Commission is conducting an Internet privacy study this month to test Web sites' policies. If the results don't show progress in protecting privacy, Congress may consider legislation, FTC Chairman Robert Pitofsky said recently.

A similar FTC review last March found that, out of 1,400 Web sites, 85 percent collected personal information about visitors and just 14 percent disclosed how it would be used.

So far, the Clinton administration has favored industry efforts at self-regulation, including the Online Privacy Alliance, a group representing American Online Inc., IBM, Walt Disney Co., Yahoo! Inc. and others.

Consumers can access BBBOnLine at www.bbbonline.org, Truste at www.truste.org, and Online Privacy Alliance at www.privacyalliance.org.

--Alan M. Wolf in Washington (202) 624-1880, through the San Francisco newsroom/cap

Bloomberg
March 17, 1999

Better Business Bureau Unit Starts Online-Privacy Seal Program

Washington, March 17 (Bloomberg) -- The Council of Better Business Bureaus' online subsidiary launched its privacy program in the latest bid by the business community to head off laws designed to protect U.S. consumers on the Internet.

BBBOnLine, sponsored by Microsoft Corp., AT&T Corp., International Business Machines Corp. and other companies, will expand its parent's brand recognition to the Internet, using a seal to let consumers know that a Web site adheres to certain privacy guidelines. The Commerce Department estimates annual retail sales on the Internet will increase to $30 billion by next year.

Clinton administration officials warn that Internet growth could be stifled by consumers' concerns over privacy and security. Lawmakers and regulators say if Internet privacy protections don't improve, Congress could pass legislation to curb how companies collect and use personal data gathered online.

``Our seal will mean a lot to consumers who know us on main street," said Steve Cole, a spokesman for BBBOnLine, first announced last May. ``Our goal is to build trust and confidence in the Internet."

Dell Computer Corp., the No. 1 direct seller of personal computers, is the only company that now displays the BBBOnLine seal, though the program has about 350 applications.

Web sites that display the BBBOnLine seal will be required to tell consumers what personal information is collected and how it will be used. The program will resolve consumer complaints and refer violations to the FTC.

Annual fees to display the BBBOnLine seal range from $150 to $3,000, depending on a company's sales. A separate children's seal will require companies to take special steps, such as getting parental consent before collecting or using data, to protect those under 13.

BBBOnLine will compete with Truste, a non-profit organization also backed by industry that launched its seal program in June 1997 and has already signed up more than 500 Web sites.

IBM, which sponsored both programs and had about $3 billion in online sales last year, displays the Truste seal and hasn't decided if it will add BBBOnLine, said IBM spokeswoman Harriet

Pearson. ``We're seeding and supporting multiple self-regulatory efforts," she said.

Consumers can find BBBOnLine at www.bbbonline.org and Truste at www.truste.org.

--Alan M. Wolf in Washington (202) 624-1880/ah

CNET News.com
March 16, 1999

BBB Web site privacy program finally arrives

By Courtney Macavinta
Staff Writer, CNET News.com
March 16, 1999, 10:05 p.m. PT

The Better Business Bureau will finally launch its Net site privacy program tomorrow, the latest in a string of industry efforts to stave off regulation and to quell conflict between U.S. and European officials over data collection practices.

The long-awaited BBBOnline privacy seal requires applicants to indicate when they gather consumers' sensitive information, how they use it, and how they protect it. Sites with the BBB privacy mark also must give Net users access to their records and let them "opt out" of giving up personal details such as name, phone number, or financial information.

Sites targeted at children will carry a different seal and must meet the marketing guidelines laid out by the Children's Advertising Review Unit of the BBB, and get parental permission before collecting data from those under age 12.

The BBBOnline will monitor sites for compliance, sometimes making random on-site visits.

"The program is about putting a trusted brand name on a Web site when they qualify under our standards for fair information practices," said Steve Cole, general counsel for BBBOnline. "This should give regulators a comfort level that the business community gets it and has done something that has teeth to it."

Self-regulatory plans have been criticized in the past by privacy advocates and U.S. officials for lacking strong enforcement. BBBOnline promised to meet this demand when it announced the program last summer.

The organization plans to collect consumers' Net privacy complaints, giving a company ten days to respond and possibly correct the situation. But if a company is found guilty of violating its privacy policy, BBBOnline will revoke the seal, make the invalidation public and possibly refer the matter to the Federal Trade Commission or other agencies.

The BBBOnline seal is similar to another well-known privacy "trustmark" on the market, TRUSTe, and the budding accreditation program WebTrust by the American Institute of Certified Public Accountants (AICPA), which represents the "Big Five" accounting firms.

Depending on gross sales, companies will pay from $150 to $3,000 per year to participate in BBBOnline. Its corporate sponsors, many of whom also support TRUSTe, have paid more than $50,000 each to help build the program. AT&T, Hewlett-Packard, Netscape Communications, and Microsoft are among the backers.

Still, even before it launched BBBOnline was lambasted by privacy groups for not exploiting its potential reach with the program.

For example, another BBBOnline program, its reliability seal, already is in place and has 2,300 participants. If a site carries that seal it means the BBBOnline has visited the company in person, among other checks, to ensure it can back up the services it is pitching on the Web.

However, Web sites that carry the reliability seal, and those who are BBB members in the offline world, will not be required to sign up for the privacy program. The organization estimates that 25 percent of its 270,000 members are on the Web. As of yet it has received just 300 applications so far for its privacy program.

"We have not at this time made a decision to require it, but we are taking steps to encourage it," Cole said. "If they qualify we are offering the privacy seal for free to reliability program members for a substantial time. We're also going to work with BBBs around the country to help them create marketing materials, while we reach out in the offline world through mailings, meetings and our Web site."

The BBBOnline program may catch on, and its brand is well known, but lawmakers may be losing patience with the industry.

Although the FTC was briefed about the BBBOnline program
and is apparently pleased with the progress, Congress
members already have introduced new bills this session to tighten computer users' privacy

protections. And tomorrow, the Commerce Department will give a status report on its lengthy negotiations with EU officials.

The European Union's strict privacy directive went into effect in October and is expected to be adopted by all 15 members countries.

The EU law will give citizens new control over their computerized personal data and prevent firms from exchanging the information with countries that do not provide "adequate" protection, such as letting people "opt out" and making clear who else will have access to the data.

The EU is dissatisfied with safe harbors proposed by the United States, which in many ways mirror programs like the BBBOnline. Among the sticking points is that the U.S. proposal doesn't give consumers adequate access to their data or proper recourse for abuses.

America Online, Walt Disney, and other companies said today that they won't endorse the plan to bring them in line with the EU privacy rules, either, according to reports.

Interactive Week
March 17, 1999

Better Business Bureau Gets Personal
By Will Rodger

The Better Business Bureau today unveiled details of its long-promised Internet privacy assurance program. Touting the effort as the most comprehensive yet devised, BBB Online General Counsel Steve Cole told reporters this morning his group will make sure that more than 300 participating companies "will say what they do, do what they say and then have it verified."

The program's launch couldn't come at a more crucial time. After more than three years of back-and-forth over the issue, pressure for new laws to protect personal privacy is mounting. Legislators have introduced dozens of bills proposing restrictions on personal information gathering in just the past year, while U.S. Undersecretary of Commerce David Aaron and European Community Director General John Mogg are due today to announce results of talks concerning data flows that leave Europe bound for the U.S. Unless the U.S. can show that American companies will voluntarily safeguard Europeans' personal data once it reaches U.S. shores, even major multinationals may be banned from routine business transactions. In short, everything from credit-card purchases to airline reservations data could grind to a halt. "Such a disruption would be a disaster of historic proportions," Aaron told attendees at the annual Information Technology Association of America policy conference.

Under the BBB plan, companies displaying the group's seal will tell consumers what personal information they collect from them and what they will do with it afterward. Company participants also will agree to let customers examine for accuracy the information they keep about them. Companies displaying the seal will be asked to submit to periodic audits, as well as to the BBB's dispute resolution procedures when controversies arise.

BBB participants also will have to guard their Internet servers against intruders, so that hackers, insiders and others cannot easily grab personal information from their systems. Companies that run afoul of these requirements will be subject to dispute resolution when consumers complain, and to providing some form of restitution when BBB panels dictate it. In some cases, the BBB may yank the seal altogether or refer consumer complaints to the U.S. Federal Trade Commission.

Dispute resolution, however, will not include fines for companies that fail to live up to their promises.

The BBB's proposal won a partial endorsement from Evan Hendricks, editor of Privacy Times and a longtime critic of industry self-regulation.

"It doesn't add up to adequacy on a national scale," Hendricks said. Even so, "they've boldly gone where no self-regulatory policy has gone before."

As well-intentioned as the program is, he said, there's no assurance it will be widely adopted; a similar program known as TrustE has only a few hundred members after nearly two years of operation.

Nevertheless, Hendricks added, the program sets out reasonable protections which could form the basis of a national privacy-protection law - an idea that many BBB members have fought tooth and nail.

"Individuals really need legal rights," he said. "What this shows companies that do this is, it's really not that hard to do."

Computerworld
March 22, 1999

BETTER BUSINESS ONLINE? MAYBE

Bureau to report privacy offenders; activists skeptical

BY ANN HARRISON

IN AN EFFORT to demonstrate industry self-regulation, the Better Business Bureau Online last week announced a privacy seal that companies can place on their Web sites to show they're voluntarily following the bureau's privacy guidelines. But watchdogs charge that the initiative — like another one before it — lacks teeth.

Web sites posting the BBBOnline seal will agree to disclose what information a Web site collects from visitors — like installing cookies or data that displays the domain name of the visitor — and to explain what it does with that data. Also, sites that rent out their customer lists to third parties must give consumers a chance to remove their names beforehand.

CEO RUSS BODOFF: BBBOnline will report firms that violate privacy rules

Dell Computer Corp. was the first to place a seal on its site last week, and 350 more have applied for one, according to BBBOnline. A similar program run by Truste in Palo Alto, Calif., is 3 years old and has 500 licensees, including America Online Inc. and Microsoft Corp.

Pricing for two services ranges from a few hundred to a few thousand dollars, depending on a site's complexity, and they operate slightly differently.

Truste monitors member sites and helps companies create privacy policies, said Anne Jennings, marketing communications manager at Truste. BBBOnline will conduct surprise audits on licensees and publicly identify companies that don't comply, as well as report them to the Federal Trade Commission for legal action, said Russ Bodoff, CEO of BBBOnline.

Before granting a seal, BBBOnline will evaluate how Web site operators secure the data on their servers and how information is moved within the company, he said.

Privacy groups are skeptical whether groups like Truste and BBBOnline can hold companies accountable for their actions, especially because they're bankrolled by major technology companies.

But Kate Delhagen, an analyst at Forrester Research Inc. in Boston, said the entrance of BBBOnline may help widen acceptance of privacy seals among smaller electronic-commerce operators. "The [Better Business Bureau] has great local penetration, and there is no reason why local retailers shouldn't support this cause and ease consumers' fears about security," Delhagen said.

Jason Catlett, president of Junkbusters Corp., a Green Brook, N.J.-based privacy watchdog group, said that as a nonprofit group, BBBOnline can't legally enforce privacy violations.

Privacy Journal
April, 1999

WEB SEAL OF APPROVAL READY

BBBOnLine, the first Web site privacy certification program with any teeth in it, has opened for business after delays in getting started.

The Better Business Bureau, an 86-year-old complaint-oriented customer service run by local businesses, will operate the on-line version. After a check of the reliability of a business and whether its privacy policy meets certain standards, BBD will provide a Web site with a logo to show compliance with privacy standards. The company must agree to submit customer disputes to arbitration (*www.bbbonline.org*). A competing service, TRUSTe (*www.truste.org*), awards its seal of approval to Web sites without evaluating the content of privacy policies.

IBM Corp., a privacy pioneer and second largest advertiser on the World Wide Web, announced that beginning in June it would not advertise on any sites without clear privacy policies, including a chance to opt-out of any secondary use of personal information.

The CHAIRMAN. Mr. Fischbach.

STATEMENT OF GREGORY FISCHBACH

Mr. FISCHBACH. Thank you, Mr. Chairman, Senator Kohl and Senator Schumer, for the opportunity to testify before the committee today regarding the protection of personal information on the Internet. I applaud you for your leadership in seeking to strike the right admittedly delicate balance between industry self-regulation and the appropriate role, if any, of government.

I testify today wearing two hats. I am the Chairman and Chief Executive Officer of Acclaim Entertainment, a leading maker of video and PC games. Though headquartered in New York, Acclaim's flagship develop studio is Iguana Studios in Salt Lake City, which employs 90 software professionals.

Senator SCHUMER. Excuse me, sir. Are you bragging about that? [Laughter.]

The CHAIRMAN. Let's not have interruptions from New York. [Laughter.]

We ought to be grateful here for the link-up, you know.

Mr. FISCHBACH. Well, it works for both of you.

I am here as Vice Chair of the Interactive Digital Software Association, the trade body representing the $6.3 billion U.S. entertainment software industry.

Maintaining communication with our customers is fundamental to our success as a business. Unlike many other businesses where the essential interaction with consumers involves a one-time transaction, entertainment software consumers expect and even rely on a continuous dialogue with their publishers. For example, buyers of our games expect us to provide them with software bug fixes, game tips, virus warnings and software upgrades.

The Internet has become a major vehicle for talking to our customers. We use it to provide online product registrations, direct download of bug fixes and updates, new product information, and online gaming services. We recognize that using the Internet to communicate with customers means we must appropriately safeguard the personal information we collect and use online.

In October 1998, the IDSA officially adopted voluntary principles and guidelines for fair information practices online. The guidelines generally conform to privacy principles proposed by the Department of Commerce and the OECD. While consistent with guidelines issued by other industry groups, the IDSA guidelines go further in three areas—access, information and children.

On access, the IDSA guidelines direct that companies give consumers the opportunity for reasonable, appropriate access to personal identity information and the opportunity to correct or amend that information. In the area of enforcement, the guidelines direct the IDSA to make publicly accessible a status report on IDSA member implementation of privacy practices, and they require that members utilize certification seals provided by third-party entities.

Finally, in the children's area the IDSA guidelines require that companies provide parents of children ages 13 to 17 with notice of online information collection and the opportunity to remove the information from the site's database. To date, 16 IDSA members, who together accounted for almost 60 percent of all games sold in the

U.S. in 1998, have posted online privacy policies as required by our guidelines or are in the process of doing so.

For our company, compliance has required fundamental changes in the way that we do business and relate to our customers. This is an important point. Business does have a responsibility to protect privacy, but government must understand that these changes often touch on the most basic and important business asset we have, our consumer relationships.

Let me tell you that overhauling our business model in this area is not as easy as it might seem when rules are first put on paper. In fact, we at Acclaim have opted to significantly limit how much information we collect on our Web site. Acclaim.net only collects and stores e-mail addressed, and only does so in three circumstances.

When a Web site visitor is subscribing to our newsletter, downloading software, or ordering something from our online store, we make it clear that we may use these e-mail addresses for a variety of internal marketing purposes, but do not sell or distribute them to any outside person or organization. We also offer our customers the ability to have Acclaim delete their e-mail addresses.

Finally, we expressly forbid children 12 and under from submitting information to us, and we will implement whatever consent and notice procedures the FTC identifies as appropriate regulations that are promulgated under this law. Our policy is posted and we hope to have a certification seal from the ESRB as soon as it is open for business, which we would anticipate by the end of this May.

Mr. Chairman, I believe our industry and my company have made important strides toward protecting privacy. But my experience in these last few months tells me that one size does not fit all. A legislative or regulatory approach probably creates great confusion. I understand the appeal of a Federal mandate, but as someone working in the trenches I suggest to you that industry self-regulation, while perhaps imperfect, is ultimately the best and swiftest way to protect consumer privacy on the Internet, while allowing Internet creativity and experimentation to flourish.

Thank you for this opportunity and I would be glad to answer any questions.

The CHAIRMAN. Thank you, Mr. Fischbach.

[The prepared statement of Mr. Fischbach follows:]

PREPARED STATEMENT OF GREGORY FISCHBACH

Thank you, Mr. Chairman, for the opportunity to testify before the Committee today regarding the protection of personal information on the Internet. I applaud you for your leadership in seeking to strike the right, admittedly delicate balance, between industry self-regulation and the appropriate role, if any, for government.

I testify today wearing two hats. I am the Chairman and Co-Chief Executive Officer of Acclaim Entertainment. I am also here as the Vice-Chair of the Board of Directors of the Interactive Digital Software Association.

Acclaim Entertainment, Inc. is a leading worldwide developer, publisher and mass marketer of software for use with interactive entertainment platforms including Nintendo, Sony and Sega hardware systems, and PCs. Acclaim owns and operates five studios located in the United States and the United Kingdom, and publishes and distributes its software directly in North America, the United Kingdom, Germany, France and Australia. Acclaim posted 1998 revenues of over $325 million. Our headquarters are located in Glen Cove, New York and Acclaim's common stock is publicly traded on NASDAQ under the symbol AKLM.

You may know some of our key internally developed brands, Acclaim Sports, Turok, and *WWF* Warzone. *WWF* Warzone, developed by our flagship studio, Iguana Salt Lake City, was Acclaim's best selling product in 1998. Our Salt Lake City Studio employs over 90 software professionals and generates several products annually.

All of our company brands are supported by significant marketing campaigns including on-line promotion. Over the last year we have allocated significant resources to Acclaim On-Line, in an effort to better service our consumers. Consumers visit our site, Acclaim.Net for product information, release dates, free demo software, Ecommerce, tips and hints and company information. Last year traffic on Acclaim.Net grew by 325 percent. In calendar 1999, we expect to generate over 50 million page impressions. In the future we plan to continue to serve our consumers online by offering new features including on-line game play through Acclaim.Net.

The IDSA represents the U.S. publishers of entertainment software games for video game consoles, PCs, and the Internet. IDSA members collectively account for more than 85 percent of the $6.3 billion in entertainment software sold and rented in the U.S. in 1998, and billions more in export sales of U.S.-made entertainment software. The entertainment software industry is now the fastest growing of all U.S. entertainment industries, selling nearly 200 million units of PC and video games in the U.S. alone, or almost two per household.

I want to spend my time sharing with you some of the lessons that Acclaim and the IDSA have learned as a result of the steps that we have taken to protect the personal information of entertainment software consumers online.

Let me start with a little context: maintaining communication with our customers is at the core of what we do. It is fundamental to our success as a business. Unlike many other businesses where the transaction with consumers is a one-time event, our consumers expect and even rely on this continuous dialogue.

Consumers expect us to provide them with software patches, game tips, and software upgrades and enhancements. They want information from us on sequels, they want technical support, they want to tell us what they think of our products, they want to volunteer to test products, and more. Consumers of online games, a growing part of the entertainment software industry, also increasingly expect us to provide online game services so they can participate in tournaments, find playing partners, or play massive multi-player games. Without personal information from those consumers, such as email address, name, and snail mail address, we cannot meet these needs; moreover, in an industry which is besieged by piracy, we need registration information to ensure that the consumer owns a legitimate, rather than pirated, copy and we need personal information from online game players to prevent players from abusing the game service or harassing other players.

The Internet has become the major vehicle through which we meet many of these consumer demands. The Internet allows us to provide online product registrations, direct downloads of bug fixes and updates, new product information, and online game services.

We recognize that our use of the Internet to communicate with our customers imposes a burden on us to put in place appropriate safeguards to ensure that the personal information we do collect is protected. This leads me to the actions that both Acclaim and the IDSA have taken to protect the personal information of consumers online.

In March 1998 the IDSA convened a Privacy Working Group to create appropriate standards for protecting the privacy of consumers on the Internet. This Privacy Working Group consisted of General Counsels, Marketing Directors, and Webmasters from nine IDSA member companies, bringing legal, business, and technical expertise to the issue. Over the ensuing eight months, this Working Group and the IDSA Board hammered out Principles and Guidelines for Fair Information Practices. The Board officially adopted these Guidelines at its October 1998 meeting, and IDSA members are expected to be in compliance by May 31, 1999. Copies have been provided to the Committee.

Developing these guidelines was not simple. It's easy to lose sight of the fact that we are talking about redefining how we relate to our consumers. From a business standpoint, this is not something we take lightly, especially not after spending years to build a sense of loyalty and trust with those who play our games. While some believe developing guidelines is a simple matter, we know from experience that even using the very valuable templates developed by such groups as the Online Privacy Alliance, the Organization for Economic Cooperation and Development (OECD), and the Department of Commerce, an enormous amount of thought must still be applied to ensure that the guidelines we've adopted for this industry take into account its unique qualities.

We believe that the Guidelines we eventually developed represent an appropriate balance between protecting the online privacy of our customers while also preserv-

ing the interactive relationship that our customers expect. As their longer title indicates, the guidelines have two elements. First, they establish a core principle to which companies adopting the guidelines must adhere. Second, they provide guidance on ways to comply with each core principle, recognizing that companies may, depending on size, practices, and resources, choose different paths to complying with the principles.

As these elements are widely recognized to be essential, the IDSA Guidelines contain principles on Notice, Choice, Data Collection Limitation, Security, Access, Enforcement, and special rules for children. With regard to Notice, Choice, Data Collection Limitation, and Security, the IDSA Guidelines are in conformance with those suggested by the OECD and the Department of Commerce, and consistent with those adopted by other industries and companies. However, the IDSA Guidelines go farther than other industries with regard to Access, Enforcement, and Children.

With respect to Notice, Choice, and Data Collection Limitation, and Security, the IDSA guidelines (1) direct each IDSA member to implement and publish online a "privacy policy" that informs consumers about its online collection and use of personal information, (2) direct that each IDSA member give consumers the choice to exercise reasonable control over the collection and use of their personal data, generally establishing "opt-out" choice as the minimum acceptable tool; (3) direct IDSA members to only collect and retain personal data of consumers that is needed for valid business reasons, and give guidance as to the breadth of personal data that should be collected and when personal data should no longer be retained; and (4) direct that IDSA members take reasonable measures to assure the reliability of personal data they collect and take reasonable precautions to protect that data from loss, misuse, or alteration, and recommend that IDSA members take reasonable steps to assure that third parties to whom they transfer the personal data of consumers will provide sufficient protection to that personal data.

As an industry which is both highly sensitive to our customer relationships, and which has a significant following among children, we spent considerable time crafting guidelines in the Access, Enforcement, and Children's areas. The result is that our guidelines in these areas, in some instances, go beyond recently enacted law and other voluntary approaches.

For example, the IDSA guidelines with regard to access do not restrict consumer access to instances of ensuring data quality. Instead, they direct that IDSA members give consumers the opportunity for reasonable, appropriate access to personal identifying information about them that an IDSA member holds, and the opportunity to correct or amend that information when necessary.

In the enforcement area, the IDSA guidelines create a detailed scheme for ensuring that IDSA members comply with their data privacy policies and provide appropriate means of recourse for consumers. They give explicit direction on internal mechanisms that should be followed, including establishment of clear procedures and specific time frames for resolution of complaints, identification and training of personnel that will ensure compliance and provide recourse to consumers, and appeals structures. IDSA members are also directed to create a system of incentives and/or sanctions, which might include bonuses, to encourage adherence to privacy policies. I believe that the vast majority of consumer complaints will be adequately and effectively addressed through these mechanisms.

But, in order to provide consumers with additional confidence that they can rely on a privacy policy, the IDSA guidelines also establish two external mechanisms for ensuring member compliance with the IDSA guidelines. First, they direct the IDSA to make publicly accessible, both on its Web site and in its files, a report on the status of IDSA member adoption and implementation of privacy practices. After the May 31, 1999 deadline for compliance, this status report will, among other things, identify the certification seal provider used by each member, include links to the privacy policies of IDSA members, and inform consumers how to access privacy practice compliance information about each IDSA member from the relevant seal provider.

Second, the IDSA guidelines *require* that members utilize certification seals provided by third party entities. Such third party seal providers must be empowered to investigate and verify compliance with privacy policies, and to mediate or arbitrate consumer complaints. You are familiar with the BBB Online program, one prominent third party seal provider. In a few months, the Entertainment Software Ratings Board (ESRB) will launch its own seal program for entertainment software companies. Since 1994, the ESRB has been rating entertainment software titles for age and content appropriateness. Senators Kohl and Lieberman have called the ESRB the best and most credible entertainment ratings system in the U.S. More recently, the ESRB has begun rating entertainment software web sites along similar lines. In rating more than 5,000 products and web sites, the ESRB has developed

a depth of ratings experience as well as terrific brand recognition and confidence among entertainment software consumers. The ESRB therefore decided it was a natural progression to build on that consumer trust by expanding into the privacy ratings arena. I'm sure the ESRB would be happy to share with this Committee details about its new seal service.

The last area of the IDSA guidelines I would like to discuss are its rules regarding children. While 56 percent of video gamers and more than 70 percent of computer gamers are over 18, the IDSA recognizes that many children use our products, and that the online collection and use of personal data from children raises a different set of concerns than exist with adults. Therefore, the IDSA has adopted a more rigorous set of guidelines with respect to IDSA members that collect information from children.

With respect to children age twelve and under, the IDSA guidelines mirror the recently enacted Children's Online Privacy Protection Act, but we go beyond the Act to create special rules with regards to children over twelve and under eighteen. If IDSA members engage in collection of personal information from these older children, the IDSA guidelines direct them to provide parents with notice of the collection and an opportunity to remove the information from the site's database.

To date, sixteen IDSA members, who together accounted for almost 60 percent of all games sold in the U.S. in 1998, have posted online privacy policies as required by the Guidelines or are in the process of doing so. IDSA is actively reaching out to others in the industry, and plans to meet face-to-face with the remaining members at our annual industry trade show next month. The IDSA also plans a series of regional seminars to help its members work through implementation issues.

Once the IDSA adopted these guidelines in October 1998, the really tough work began. While drafting guidelines to cover companies of assorted sizes, resources, practices, business structures, and sensitivity was challenging, it is an even greater challenge to implement them. I tell you that based on real world experience. Think tanks, interest groups, government agencies, and congressional committees are laboratories; what might seem workable in the lab is not always practical outside of it.

Acclaim has been actively trying to implement the IDSA guidelines for several months. If there is any one message I would like to leave you with today, it is that even modest rules on online collection and use of personal information often require fundamental changes in the ways companies do business and in their customer relationships. It is important to remember that for entertainment software companies this is an area vital, as folks in DC like to say, "to our national interest." Anything we do which affects our interaction with customers is a significant business issue. As I noted earlier, our customers expect an ongoing relationship, and the effort to meet these expectations and protect their privacy is not an overnight process.

In the last few months, Acclaim has conducted an internal review of our Web sites and the way they collect and use personal information from Web site visitors. We then worked with the IDSA to understand the guidelines and the changes we would have to make in our business practices to comply with the guidelines. We have posted a privacy policy on our Web site, and hope that the ESRB Privacy Program will soon be operational and thus able to review our policy and practices. If the ESRB requires further changes to our privacy policy and practices, we will have to devise ways to implement these changes.

The privacy practices that Acclaim developed as a result of these efforts are, I think, pretty straightforward: we have opted to significantly limit how much information we collect on our Web site. We only collect and store email addresses and only do so in three circumstances: when a Web site visitor is subscribing to our Newsletter, downloading software, or ordering something from our online store. We make it clear that we may use these email addresses for a variety of internal marketing purposes, but will not sell or distribute these email addresses in any way to any outside person or organization. We do offer customers the ability to have Acclaim delete their email addresses from our databases by emailing our Webmaster with the word "remove" in the subject header of the email. Finally, we expressly forbid children twelve and under from submitting information to us, and will implement whatever consent and notice procedures the Federal Trade Commission identifies as appropriate in regulations promulgated under the Children's Online Privacy Protection Act.

As I stated, this "simple" Acclaim policy resulted from a very difficult process of figuring out how to apply the IDSA Guidelines to Acclaim. I will just to throw out a few scenarios to demonstrate the difficulties we faced when we tried to implement information collection and use limitations.

The words "provide reasonable, appropriate access" seem simple. But what do they mean in practice? Suppose a consumer calls Acclaim in New York and asks

for all information that all our operating units have on them? Acclaim New York and Iguana Salt Lake City have separate databases. Is it reasonable to give the consumer the information we have in New York and direct them to make other calls to ascertain the information held by other units? I'm sure the consumer would regard that as a nuisance. But the alternative would be for Acclaim to centralize all its databases. That is a very costly and complicated undertaking. Moreover, it raises privacy issues of its own since we would now have greater ability to develop profiles of individuals by aggregating all the data held by our individual companies.

In the children's area, implementing the requirements for parental consent and notice are extremely difficult. For example, what does Acclaim do about the personal information it has collected from consumers for several years through offline registration of different products, such as our NFL Quarterback Club series? We collected information from registrants of NFL Quarterback Club '98 so that we might send them software bug fixes or information on the 1999 version. However, we never collected information on the age of these registrants, so now we are in a bind. What if some of these registrants are twelve and under? Are we breaking the new federal law, because we do not have parental consent to do so, by contacting them via email to inform them that their software is buggy? Alternatively, are we violating the IDSA guidelines by sending the same email to a seventeen-year-old registrant because we do not send his parent notice of this contact? This could be solved by grandfathering in previous collected information, but for now it remains a troubling area of uncertainty.

I mention these challenges not as an excuse for inaction, but a warning that what seems simple in principle can be devilishly complicated in reality. I believe IDSA's guidelines do protect consumer privacy while allowing entertainment software companies to maintain an interactive relationship with customers and to continue to experiment with business models on the Internet. But they may not be for everyone in the private sector. They are specifically crafted to meet the privacy expectations of entertainment software customers and the business needs of entertainment software companies. So our industry has made important strides toward protecting privacy. But my experience these last few months developing a privacy policy which works for Acclaim tells me that a 'one size fits all' legislative or regulatory approach is a recipe for confusion. Industry self-regulation, while imperfect, is ultimately the best and swiftest way to protect consumer privacy on the Internet while allowing Internet creativity and experimentation to flourish. Thank you.

The CHAIRMAN. This has been an extremely interesting panel. I have to momentarily go meet with the Russian foreign minister on a very important matter and so I may have to leave before I can finish my questions, but I am going to try and come back.

Let me begin with you, Mr. Sheridan. It is no secret that the Internet provides a new, valuable medium for merchants, as they are able to use the network to collect personal information about consumers. Some of the obvious methods by which commercial Web sites collect personal information include online surveys, registration pages, contests, and application forms.

However, it is my understanding that sites also collect personal information, using technologies that are not obvious to the particular Web surfer. There has been a lot of confusion as to exactly what some of these technologies are and how they work.

Could you please explain to us what a, "cookie," is and how it works?

Mr. SHERIDAN. It is fattening.

The CHAIRMAN. It is fattening.

Mr. SHERIDAN. Well, a cookie, as Mr. Berman mentioned earlier, is not an evil thing in and of itself. When you go to a page and fill out a form and you have put in what you are interested in, and magically next time you reappear at that page your preferences are known on what kind of news you would like, what has been set there is some data about you and what you are interested in and that is a cookie, in a simple way.

It is also used when you go to buy a book at one of the online bookstores, for example. It has your credit card, shipping and all kinds of other information, and the nice thing is you can click there and just buy the book. The potential downside is that information is being used to help you and sometimes it is not clear how it is being used once it is in the system.

The CHAIRMAN. If I understand you correctly, basically, a cookie is the technology that extracts information without the consumer knowing about that information.

Mr. SHERIDAN. Generally, the cookie is set through information gotten by the consumer. Of course, it could also just log the fact that you were there and your address, too. It is a two-edged sword.

The CHAIRMAN. Does this allow the Web sites to track which pages a consumer views and for how long?

Mr. SHERIDAN. Well, the cookie doesn't necessarily do that, but inside of their system, depending on the site, there are ways in which the user can be essentially followed. They would know what they had clicked on and what their preferences were, then use that often to recommend something positive, such as a recommendation for a book that they think you would be interested in, based on what you had clicked on.

The CHAIRMAN. Is there technology available, or do Web browsers allow a consumer to set his or her computer to prevent cookies from being placed, or at the very least give the Web surfer notice before it is placed in the computer?

Mr. SHERIDAN. Web browsers from early on in the development of this technology have allowed the user to turn off cookies or to ask for notification when one is being asked for.

The CHAIRMAN. I see. I want to thank you for this because it is helpful in educating the public in two ways. First, by letting them know how information could be extracted from them and, second, by informing them that they do have the power to control how some of these technologies are used through the use of technologies that they may already have on their laptops. So I think that is important that we establish that.

Mr. SHERIDAN. Yes, it is.

The CHAIRMAN. Now, Ms. Borsecnik, as an Internet service provider and a portal, you may have an interesting perspective to add. Does AOL use cookies on its Web sites?

Ms. BORSECNIK. AOL does use cookies on its Web sites. We use cookies to identify whether a customer has been there before. What we do is we can personalize a page someone sees based on the fact of whether they have been there before. So, for example, the first time they come we may offer a degree of help, a degree of explanation about the site that is not required on subsequent visits, things like that.

Our system automatically collects a lot of data, some of which is required for us to run our business and some of which isn't in a personally identified way. So when we collect data of where people go online, we store and use that data in a way that anonymizes it and doesn't allow for us to connect that data with a specific user and we review it in aggregate. So we may know, for example, that "x" number of people have visited the personal finance area, but we couldn't say that you were a visitor to the area that day.

The CHAIRMAN. I see. Mr. Berman, I need to run and I am appreciative that Senator Thurmond is here to spell me off, but it appears that some uses of cookies are legitimate and help to create a more efficient Internet. However, it also seems that these cookies could be used by some bad actors for purposes that certainly would be suspect. Maybe you could shed some light on what some of these less desirable uses of cookies are and what type of Web operators use cookies in these improper manners.

Mr. BERMAN. Well, it is very difficult to make a judgment like that. Anyone who is using information in a way which I did not consent to—I go to a site, I think I am just browsing. They collect information about me. Then they may have marketing information and they are selling something to me. I don't like it. So it is a relative judgment by the consumer.

I think that you are onto the right answer, which is that consumers ought to know that a cookie is being placed, in other words that information is being collected. There are mechanisms now in the browser which allow you turn a cookie off. There is even more advanced technology, such as the P3P platform, which the World Wide Web Consortium is working on with other industry and privacy organizations which will allow you to set your browser and state your preferences about what you want collected or not collected about you, and that will help to turn a cookie off or keep you away from sites that are collecting that information. The consumer can be put into a position to know what is going on.

The CHAIRMAN. Mr. Wladawsky-Berger.

Mr. WLADAWSKY-BERGER. Yes. If I may add, Mr. Chairman, I think that all of the self-regulation concepts have at their heart an empowered consumer, and that is why what we always want is three key principles—notification, choice and recourse.

Notification means that the consumer, the person that you are interacting with, always knows what is happening, what information you are collecting, what it is going to be used for. Choice means that if they are happy that it will be used for good things, they are happy to let you have it; otherwise, if they don't know or choose for whatever reason not to give it to you. And recourse means that there is a way, if you feel that you have been wronged, to take recourse, like contact BBBOnLine or some other mechanism, or in some cases the Federal Trade Commission.

So I think those are the key principles, and then within those principles there are a lot of technologies that can do a lot of good, but if misused, then they can be used wrongly.

The CHAIRMAN. Well, thank you.

Mr. BERGER. I just wanted to add one point, which is the most difficult issue to resolve is the recourse issue. One, getting everyone to put those notices up and tell you what is happening with information, but with the millions and millions of Web sites and the new ones coming online, the self-regulatory efforts that are going on are really important. And AOL and Microsoft are doing a good job in terms of trying to move along toward self-regulation. We do have to raise the issue of the bad actor and the small Web site and what the recourse is there. That is not clear, but it is not easy to write because the violations have to be spelled out.

The CHAIRMAN. Senator Kohl, let's turn to you. I apologize to you that I have to leave for that meeting, and I am not sure I can get back. But if not, Senator Thurmond will finish the hearing. Thanks so much.

Senator KOHL. Thank you, Senator Hatch. I have a single two-part question for the panel, starting with Ms. Borsecnik. Are you all worried that the worst actors in your industry, the people who do not respect privacy, will undermine your efforts at self-regulation, and that Congress will legislate on the basis of anecdote in a way that neither makes good sense nor good public policy? And if you are worried about this, doesn't it make sense to consider a commission which may preempt some of the worst legislation and, even better, bring together industry, government and privacy experts to establish a balanced approach to privacy protection?

Ms. Borsecnik.

Ms. BORSECNIK. Do we worry about it? Yes. Privacy is a real concern to our customers; we hear it on a daily basis from them. And we do worry that there are bad apples out there,tentially, just like in the days when the Senator was talking about being afraid that criminals would use cars to get away from the scene of the crime.

But we worry more about legislation activity that is too quick to put a stake in the ground at a time when—you have heard from us all that this is a nascent industry; things are moving so quickly. Maybe I am just a poor predictor, but at any point in time I have a hard time knowing what my business is going to look like in 6 months, much less 6 years.

And not only is the technology moving so quickly, I have found that customers' demands are progressing along with it. So to take a snapshot at any point in time when the industry is in its infancy and say this is the right solution, this technology is the right solution, I think I worry that that will be viewed as short-sighted in retrospect.

In terms of a commission, we believe that an open and public dialogue is an enormous help on this issue. Even incidents that have happened, I believe, in the end have helped the industry realize that more attention needs to be focused on it and have resulted in some of the activities you have heard about here today. So we are very much in support of that kind of dialogue, particularly in areas that need particular attention, like kids' privacy and health care and things like that. A one-size-fits-all solution is definitely something that we would be concerned about that could stymie our business.

Senator KOHL. Mr. Sheridan.

Mr. SHERIDAN. Well, to address the first part of your question, yes, I think we all worry about it, both individually, those with kids who have to deal with it everyday, and also because frankly it hurts our business if this trust is broken down.

We believe that the right approach is one that does not try to do everything at once; again, as my colleague here had said, a snapshot in time. And the time frames on the Internet are very compressed; things happen very quickly. And what we would be concerned about is any piecemeal, in-time solution that doesn't take into account the fast-moving nature of the Silicon Valleys of this country, and there are many of them, which are really an American

miracle of competitiveness, job creation and wealth creation. It would be our concern that that would be derailed by government intervention.

On the second part of the issue, we would welcome an open, balanced approach that is structured to represent this position. And if that were to occur, I think we would support it.

Mr. WLADAWSKY-BERGER. Senator Kohl, I agree with my colleagues that the Internet and all the applications that it is helping bring about—it is too young, too complicated and too fast to know at this time what to regulate. It is just very hard when we don't have enough information because it has only really been around, in this explosive way it has taken off, for the last few years. And it feels like every month, something brand new happens. The fear we all have is we can regulate something now that 2 years from now will just look quaint. Why did we do that when technology went way beyond that, or the marketplace?

Now, when things are moving so fast, definitely research and dialogue are more important than ever. Chairman Hatch mentioned when he introduced me that I am a member of the President's Information Advisory Technology Committee. We just submitted a report; it was just printed last week. And we recommended a doubling of IT research over the next 5 years, especially research on long-term strategic issues, and we called out specifically privacy issues as areas that should be aggressively funded because the more we understand the problem, the more we study it, the more we can then have the right approaches to getting privacy to happen. I think your idea of a commission is a very sound one. It is in the spirit of understanding and getting more information, and we would be very happy to work with you to see how best to make it happen.

Senator KOHL. Mr. Berman.

Mr. BERMAN. I certainly support the idea, particularly if it has a time frame and some very specific questions about remedies. The last privacy commission 20 years ago really did get out of the one-size-fits-all and looked at the particulars of different industries and the technology. In the absence of OTA and all of that background, this would be very helpful.

In the CDA legislation on child decency, Congress passed a second statute. It is now being enjoined in the courts, and they added to that statute a commission to study the issue about what was the best way to do it. They passed the legislation before they finished their commission work. Now, the commission is going to start. I think the better way to do it is to have the commission and then pass the legislation. So that would get it right for once.

Senator KOHL. Thank you. Mr. Bodoff.

Mr. BODOFF. I think there is a variety of ways of answering that question, and let me take two approaches. First of all, when we deal with bad apples, the first concern always has to be companies who don't post any privacy notice at all. If we do our job correctly in the self-regulatory area and we get out there and we educate consumers to look for privacy policies, the marketplace is going to drive companies to put privacy notices on their Web sites.

If a company has a privacy notice and violates it, through a self-regulation process and working closely with the Federal Trade

Commission and other regulatory organizations, those can be acted upon as deceptive trade practices. But a lot of talk is on the bad apples, and in our extensive experience looking at the Internet, our greater challenge is a lot of the new, smaller businesses coming online that we wouldn't describe at all as bad apples, but they are coming online with lack of sophistication and experience of how to operate on the Internet.

And it really is critical for business organizations to come together and educate these businesses on good practices because our experience is when we reach out to these companies, we have very, very good compliance with companies responding and wanting to do the right thing.

Senator KOHL. Mr. Fischbach.

Mr. FISCHBACH. Our business has really changed and will change dramatically over the next 4 to 5 years. I mean, we started writing software that was costing us $25,000, and some of the people in the back of the room probably played some of those games. But, today, we will spend anywhere between $3 and $6 million to write a title. We will spend over $100 million on R&D.

The competitive nature of our industry—it is the fastest growing portion of the entertainment business—puts everybody up to a much higher standard and really does eliminate a lot of the bad apples just because they can't afford to compete or they can't afford to participate in the organization or the association.

The industry itself is a relatively new industry. Our association is relatively new, but the steps that we have taken in order to self-regulate, I think, are to be looked at and commended. When it was asked by Congress whether we should create a rating system for our organization or not, as you know, Senator Kohl, we went ahead and did that, and we have done it very effectively and we have virtually 100 percent compliance within our industry.

We have taken the same steps with respect to our Internet sites and our Internet activities. We do think it is an issue. We are being very proactive. The companies in our industry participate on one side from Sony, which is a multi-billion-dollar company, to some very small companies. So the way that those rules will become enforced and how quickly we can have them adopted by our members may be different. It may not be quite as quick as Congress would like, but we are all moving in the right direction.

Virtually all of the companies in our association that have any kind of public presence at all, whether they be public entities or just basically marketing their products to the public as a whole, have taken an aggressive action with respect to this. So I think with respect to our industry self-regulation will work and has worked.

Mr. BERMAN. May I just add to my comment?

Senator KOHL. Mr. Berman.

Mr. BERMAN. A commission should be tracking ongoing efforts to see whether they are effective. In other words, it should not be let's all stop and study this, because there are some very important efforts in technology and self-regulation, and even legislation at the State level that ought to be looked at in terms of whether they are effective, and if they are not, what are the alternatives, and report back to Congress and to the administration.

Senator KOHL. Ms. Borsecnik.

Ms. BORSECNIK. One follow-up point is that represented here today are some of the more influential companies in the Internet industry. And as such, we have a great deal of responsibility and influence on other players. We have mentioned a couple programs today, including AOL's Certified Merchant program, IBM's advertising program, in which we have the ability to influence that sphere of business contacts and partners by only engaging in business contracts that require our business partners to follow our privacy policies or privacy policies of a standard set by BBBOnLine, or only allocate advertising dollars to those sites that agree to comply with that. I think that that is having an enormous impact, also, on the proliferation of privacy policy sites on the Web.

Senator KOHL. Thank you all.

Senator THURMOND [presiding]. Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman. One of the things I have been concerned about is the different privacy policies of different companies. I look at Web sites and while many various companies have policies, it gets kind of confusing because they are so different. Some sites reserve the right to change their policy, but only a few explicitly state that a change in policy will not affect what they have already gathered. And the fact that they may just suddenly change their mind is a little bit puzzling.

I looked at one I have got here from Polaroid. It says, "we reserve the right to change this statement at any time" on what they do. It says that they collect aggregate and user-specific information on what pages consumers access or visit. I consider myself somewhat Web-savvy, and I am sure that the Web master finds this perfectly clear, but I am not quite sure what it is they are finding out. In any event, they say they can change that any time they want anyway, so it probably doesn't make any difference what it is they are finding out.

In fact, I saw one, Purina, which goes on at great, great length about it. It is very specific, very legalistic. It looks like a corporate merger proposal. Then we have another one, though, that I do kind of like, Super Stats. They give you the legal line and then they put in parenthesis, "translation: we don't see or give your info to jerks who want to send you a bunch of junk mail." That, I like. [Laughter.]

You know, I am a lawyer, but that one I can understand and I think it is kind of nice.

I am not suggesting we sit here and impose a uniform privacy policy, but how do we reduce the confusion for consumers without us standing up here and saying here is what it is going to be? I mean, how do you do it in such a way that I go from company A to company B, to a travel agency, to this, to that and the other thing, and have some idea what the consistency is?

Mr. WLADAWSKY-BERGER. Senator, that is one of the reasons to make it very simple for a potential customer to see the practices that we all support so strongly—the seal programs like BBBOnLine or TRUSTe. The hope is that when you go to a site and you see a seal program that you trust, it is like buying, let's say, an electric hair dryer, seeing that Underwriters Laboratory——

Senator LEAHY. I don't use a hair dryer with my hairline, but I understand what you are saying.

Mr. WLADAWSKY-BERGER [continuing]. Or some other electric appliance, and it has Underwriters Laboratory. They have a good reputation. At least a base level of good practices has been followed.

Now, it is all very new. TRUSTe has been in operation about a year, 2 years now, and BBBOnLine just started. So we don't have enough information whether that will be enough. That is certainly the hope we have for the seal programs, to make life much easier.

Senator LEAHY. I have said this to your company up in Vermont: I feel, as I said earlier today, too, that good privacy policies are good business policies. I think what IBM did in your decision not to ship the Pentium III chip with the built-in serial number activated and in your decision not to advertise IBM on Web sites without posted privacy policies is very good and I hope that produces results. But I also hope that what it might do is be a kind of a corporate example that others will follow.

Mr. BERMAN. Senator.

Senator LEAHY. Mr. Berman.

Mr. BERMAN. I think that the seal programs are attempting to make some consistency across the Net in terms of expectations so that if it is a Good Housekeeping seal of approval or BBB, you will have some sense of what the parameters of those privacy policies are.

We are very much in favor of a technology step, which is the development of what is called a Platform for Privacy Preferences, which would allow you, every consumer, to set what your preferences or your expectations of privacy are as you go shopping and going around the Net. And it will only go to sites that are consistent with your preferences. And if it is inconsistent with your preferences, that side would have to negotiate with you. If they want more information from you and you don't want to give it to them in your browser, they would have to explain what the big deal is and why they are giving it to you.

I think that is absolutely essential because there is no way that the consumer is going to be able to read, let alone offline, but online, all of these policies. They need ways to make it seamless as part of their Web experience.

Senator LEAHY. Well, I know if I get my Internet through the phone company or the cable company, either under 47 U.S.C. Section 222 or Section 551, they have to give me a very clear understanding of how the information might be used. But if you are going outside that, AOL, for example, works very hard at protecting it, but that is still going to be a corporate policy, not a legal policy.

Mr. Bodoff, you were trying to say something there. I mean, what I am saying is I want to know, if I have a certain expectation under one way of having it provided, how do I get a similar expectation under another one, because most people have an expectation of privacy and may not realize that it may vary considerably where they are.

Mr. BODOFF. Well, I think one of the most important aspects of the program that we have just launched was the development, through the effort of many companies and privacy experts working

together, of what we would call a series of best practices. In a sense, it is a road map, and any company who is applying for our seal and they go through their process, they have to evaluate their privacy policy against these best practices.

So the issue that you started with, Senator Leahy, would be addressed in the criteria in our program. Each of the companies that have been approved to date in our program have had to make adjustments to the processes. So what is going to happen is as more and more companies go through these self-regulatory processes and match their own efforts against best practices that have been developed, we are going to see improvements in privacy policies throughout companies, and that is small, medium and large. And I think it is going to be very positive for the Internet and very positive for consumers.

Senator LEAHY. But are you saying that it should be done by policy and not by law?

Mr. BODOFF. We are a self-regulation organization. We believe we have laid out models that have been developed in consensus environments that really point to excellent practices that should be included in a privacy policy, and we have given the road map for companies to follow.

Senator LEAHY. But the industry seemed to say they weren't good enough or fast enough last year when they supported the Children's Online Privacy Protection Act. They said we had to have a law. The Federal Trade Commission, I think, yesterday proposed the rules for implementing that new law which prohibits Web sites and online services from collecting, using or disclosing children's personal information.

Why shouldn't industry support for the Children's Online Privacy Protection Act be taken as an admission that self-regulation has serious limitations? Ms. Borsecnik.

Ms. BORSECNIK. I think there is an obvious and real concern about children that requires even more sensitivity, perhaps not the patience to wait as the policies evolve. Therefore, we were very supportive of those efforts in the area of children because there is just a certain extra added degree of concern that you need to apply to kids under the age of 18.

In terms of the privacy seals——

Senator LEAHY. But let me just stop just for a moment. I do Internet chats almost once a week for the different schools around my State. I find it very exciting, especially when I see the quality of what the kids are asking, oftentimes better than the quality of some of the questions that we get in debate around here.

But I have no way of knowing what their age is. I mean, the school will tell us when they come on, but I wouldn't know otherwise. I don't know whether they are under the age of 13 and subject to the new law or not. I mean, how can you possibly do that?

Ms. BORSECNIK. How do we know that? Well, at AOL we encourage parents to set up separate accounts for kids that are set up specifically with controls in place for children that limit their ability to interact online in adult areas. And, in fact, that effort has been very successful. At this point, over 75 percent of households with children in them that are AOL users use parental controls for their kids' accounts. So we have worked really aggressively in that

area because we do believe that added care and protection is required for kids online, and added supervision.

Senator LEAHY. I cut you earlier in your answer.

Ms. BORSECNIK. I am sorry. I was referring back to the point someone made earlier about these Good Housekeeping-equivalent seals. They are very helpful, we have found, among our members in helping convey that sense of security. What we found when we started looking at our privacy policy and rewriting it a year ago was we are throwing around terms that we assume other people are comfortable with, even things as simple as "notice" and "choice." You know, we are drinking our own bath water.

When you talk to customers, they want to know, are you giving out my phone number? Are you giving out my screen name? Are you following me around where I am going online? You know, really basic questions that anybody would be concerned about, and so we found that it is absolutely essential that privacy policies need to be stated in very plain English.

Furthermore, they need to be available in an area that is easy to find online. When a customer first joins AOL, they see the privacy policy right when they are signing up to become a member and giving us their credit card. So everything that we can do and require our business partners to do that educates consumers at a really very basic level is necessary, and I believe the seal programs help in that regard, too.

The CHAIRMAN. Mr. Berman.

Mr. BERMAN. Senator, I think that the Child Protection Act, which we supported and worked on, and your mention of the Cable Act, is a very good example of what we are facing here. It would be great to just pass the Cable Act for the Internet, but as you know from the CDA experience, this is not just a cable network. It is very different. It is cable, television and everything all piled together. So trying to figure a one-size-fits-all across the Internet is very difficult to do.

What happened in the children's area is there was a clear set of concerns. It was an agreement on what was wrong, that it was inappropriate to collect that information on children. There was an effort to define what was a kid's site versus an adult site to hone in on that, and giving the FTC the flexibility to try and implement it in a way that balanced commerce, privacy and First Amendment rights. It had the element so that it was over-burdensome.

I think that the real worry of Congress stepping in is not that they couldn't set the right rules, but that the privacy rhetoric and the demands could be counterproductive by passing an overall one-size-fits-all statute. I think that is the concern, not whether legislation ultimately is needed.

Mr. FISCHBACH. In our industry, I mean we will move to electronic distribution of software. I mean, that is evident. In the next 4 to 5 years, 30 to 40 percent of our revenues will come from electronic distribution. Our consumer expects us to talk to him, whether he be 12 or he be 24 or he be 36. And unless he tells us what his age is, we won't know that.

But we have a real issue with how to communicate, how to give him patches, how to tell him how to handle certain issues, because they will come and they will talk to us on the Internet. We have

a Web master that goes back and forth. You can come to the site and you can find out about the products that we have or about the forthcoming products. We will sometimes send a notice and we will announce new products to him.

But the basic information we are collecting is just an e-mail address, at most, and very, very limited use of it. But it does create a question of how we deal with the child under 12. And I think in our industry, about 30 percent of the software is sold to children under 12 years old, and the balance is sold to adults or those over 12. So it is a real issue for us, and not one that I think legislation——

Senator LEAHY. It is also one where parents have got to start paying a lot more attention. You can't just simply say the companies and the Congress are going to do it. I mean, parents are going to start spending some time in finding what their kids are looking at off the computer, where they are going and how they are doing it.

Mr. FISCHBACH. And we came together as an industry and we spent about 6 months trying to hammer out a policy that we have agreed to as an association, and then giving that policy to another board to enforce what works with the seal. So there is a check and a balance that exists within the system, with penalties that go along with it, and a way for people to become notified if a particular company isn't following the particular protocols.

The CHAIRMAN. Thank you.

Senator Thurmond.

Senator THURMOND. Thank you, Mr. Chairman. I am pleased that we are holding this important hearing today on privacy and the Internet. I commend Senator Hatch for his leadership in this matter.

Consumers are concerned about privacy. A Business Week magazine poll has said privacy is a major reason many consumers who are not using the Internet have stayed off. Therefore, this is an important issue. At the same time, I am concerned about government regulation being the solution. I am pleased that we have many industry representatives here to discuss their efforts to advance Internet privacy. I share the view of Senator Hatch that self-regulation is better than a detailed legislation mandate, and I am glad to have all of you with us today.

Now, I have a question I would like to ask, and any one of you can answer it if you want to volunteer. When we talk about Internet privacy, there are a number of different consumer concerns that people talk about. We hear that consumers are concerned about the collection of personal data and that this affects their participation in electronic commerce.

Based on the information you receive from your customers, and based on your experience in this business, I would like to hear from you what you believe to be some of the leading privacy concerns of consumers. What is it that consumers are concerned about that is keeping them off the Internet?

Let's start with you, Mr. Fischbach, I think, and I would like to hear from any of you that care to express yourselves.

Mr. FISCHBACH. I think the principal concern of the consumer is how is the information used; what do you know about me, and how

can I stop you from using it from time to time if I don't want you to use it. In that regard, we have been pretty proactive in explaining to the consumer how we use the little information that we collect and how he can take his information off our list and how we clean our list from time to time so that we can basically deal with his issues.

Senator THURMOND. Does anybody else care to comment?

Ms. BORSECNIK. I would like to comment. Our customers tell us three major concerns, as well as others, but the three major ones are, first of all, I am concerned about the security of my data online. One of the obstacles to e-commerce is concern about whether or not, when I enter my credit card and transmit it across this unknown network, whether it is safe and secure. And our customers tend to associate those security issues and privacy issues all together. To them, it is just one sort of vague concern.

The second area we get a lot of concern about is are you tracking where I go and what I do online. Specifically, it is none of your business whether I am researching some health care issue for my family. So there is a lot of sensitivity there.

And then, finally, the question we get a lot is what of this information do you share with anyone else. As our members establish a business relationship with us, they know and agree that certain information we collect we need to use for business purposes. We need their credit card information, we need their mailing information. But they are very concerned about our practices in regard to how we share that with third parties, whether they be private industry or the government. So those are issues that we address very specifically in our privacy policy and give our customers choices about opting out of.

Senator THURMOND. With all the recent media attention to online privacy, many groups are advocating that we develop legislation imposing privacy standards for the Internet. In your written testimonies, most of you believe that broad Federal legislation to regulate the Internet at this time is premature.

As someone who has been dealing with both the policy and business implications of privacy in the real world, can you tell us what problems would occur if broad Government regulation were imposed for privacy on the Internet? I call for a volunteer. Go ahead.

Mr. WLADAWSKY-BERGER. Senator Thurmond, the biggest concern we have is that it would make it very cumbersome especially for the smaller businesses we all have a hope to attract into the networked economy to get on. The larger companies—IBM, AOL and others—could adapt to it, and we can afford the expenses of what it takes.

But for all of us, the biggest promise of this information revolution is reaching out, connecting everything, reaching everybody, businesses of all sizes. And we want to make it as easy for the businesses to get on and participate. As one of my colleagues at the table said before, the vast majority of small businesses want to do the right thing. They just don't know because they haven't used these technologies before. And we worry that if we have excessive regulation at this time, before we know what is needed, it will detract quite a number of them and that will not be good for them.

Senator THURMOND. Mr. Berman, do you want to comment?

Mr. BERMAN. Yes. I think that on one extreme is self-regulation will solve this whole problem. That is just not going to happen. On the other side is there is something called excessive legislation, and I think that I would agree with you. You were talking about the European model of a big data protection board sitting on top of the Internet.

But I also think that it is possible, and it is not a one-size-fits all. But within those parameters, there is something less than excessive legislation and more than self-regulation which Congress ought to look at it, which is to try and figure out what the differences are between the different sectors on the Internet, create safe harbors there, create remedies that work, bring that down to concreteness. That is not an impossible task; it is absolutely an essential task that Congress do it and move.

And I think that the IBM's and the AOL's and the IDSA's will be the flagship and set, I think, the good safe harbor standards about what is good behavior on the Net. But for the millions of Web sites that are not going to comply with BBBOnLine, are not going to join any seal program, have no incentive to do privacy, I think public policy requires that Congress address that issue.

Senator THURMOND. Thank you.

Ms. BORSECNIK. One other point. We keep referring to the Internet industry, and the truth of the matter is the Internet is not an industry. The Internet is a medium and the Internet touches every single industry. So when you think of it that way, everything from A to Z—the travel industry, the personal finance industry—you know, every piece of commerce, every business is moving online in one way or another. It gives a good perspective of the complexity of regulating an environment in which clearly one size can't fit all.

Mr. SHERIDAN. From our point of view, the issue is how is it that it is not immediately out of date in something that is moving this fast. The Government isn't known for its own speed, and our concern would be that a proper balance would absolutely have to be struck. And our concern is it is a snapshot in time again.

And the other one is just plain old confusion; it would be a different kind of confusion. How do we avoid confusing people additionally with a great deal of new regulations? That would be another one of our concerns. How does this not turn into a mess and a slippery slope if we do this and then all kinds of regulations follow and build on it, because once it is written in, it is very unlikely to ever go out.

Senator THURMOND. Thank you.

Mr. BERMAN. May I respond to that?

Senator THURMOND. Mr. Berman, did you want to say something?

Mr. BERMAN. I just want to respond to that. I think that, yes, there are very serious concerns that you could, you know, bollux up the Internet, and my organization shares those concerns. And a rule could be obsolete tomorrow, but there is no reason why you cannot have the flexibility to try and figure out a process which recognizes the flexibility, the changing nature of the Internet, and tries to get going on these problems.

I think that one of the confusions out there now is that no one knows what the rules are, whether they are simple or complex.

And I think that consumers are staying off the Internet because they don't know whether there is any privacy out there, and there are a lot of companies that don't know what their liability or exposure is, or what is coming down the pike. So it is very difficult to plan for privacy. Getting some simple rules and simple remedies, not complex and excessive, might help the Internet so that it would know where it is.

Senator THURMOND. Mr. Fischbach, in your testimony you address some practical problems with implementing effective privacy practices. I think it would be very helpful to us as policymakers if you could share with us some specific examples of the problems that have occurred.

Mr. FISCHBACH. Well, databases are probably the easiest one to point a finger at. In terms of where we have collected information in the past, we have been in business for a dozen years or so and we have collected information from our consumers based on registration and warranty cards that we compile on a database and from time to time sift through. We also have operated several different sites from time to time where we collected information from consumers, for whatever the reasons were, that would talk to us.

When it came to the question of how we deal with the term "access" and how we define what we are supposed to do with the consumer who comes to us and says, OK, I would like to know what kind of information sits in your database about myself, does that mean as a company that we have to go through the simple record of the site that we now operate and say, OK, we can sift through that pretty quickly?

Does it mean that we have to go through the other databases that we kept and say, OK, now we have to collect that information to find out what we know about you? Or do we go even to a third place where we have collected these warranty cards from our consumers who registered with us for products? And we ship about 15 million boxes a year, so we have lots of cards that we have been dealing with over the last 12 years or so.

And the question is how do we interpret that. We interpreted that language to say that we would use reasonable efforts to come back and provide whatever information the consumer was asking for to tell him what we knew about him that sat in our database.

Senator THURMOND. Mr. Bodoff, some——

Mr. BODOFF. Well, I probably could share some of these—I am sorry.

Senator THURMOND. I just started to ask another question. Did you want to comment on this?

Mr. BODOFF. The only thing I was going to add to that from our experience and in the development of our process and hearing many companies going through it is that having the opportunity to revisit and look at what is identified as good practices, large companies with multiple divisions are finding surprises. That is going to happen. The positive thing is moving to address them. Having information being maintained on a Web site by a lot of different business units, it has to filter down to these large, diversified organizations. So as they move to improve their privacy policies, I think organizations are finding challenges in front of them, and the positive thing is the way that they are responding to them.

Senator THURMOND. Mr. Bodoff, some of the witnesses have noted the industry seal programs, such as BBBOnLine and TRUSTe, to address self-enforcement. Can you explain how BBBOnLine works and how BBBOnLine is different from other seal programs?

Mr. BODOFF. Well, as I mentioned earlier in my testimony, we have an 86-year history in self-regulatory activities. Our program, we believe, goes much further than any other privacy seal effort on the Internet. It is extremely comprehensive in that it does not look at just the privacy notice. It looks at the entire information practices within the company and it evaluates whether the company has the processes in place to be able to live by the privacy notice. And that is very, very important because that is where we are getting feedback from the companies.

Now, when they are asked to measure their processes against the policy statements that they are making is where the rubber hits the road and when they really realize whether indeed they do have the processes in place. So I think it is the comprehensiveness, the way our program has been described, the name recognition. One of the things that we bring to the table is very quick public confidence levels in a seal associated with the Better Business Bureau name because of the public trust level associated with our organization.

Senator THURMOND. I now have to leave for another engagement. I wish to thank all of you people for coming here and testifying and giving us the benefit of your good advice.

I thank you, Senator Hatch, for the good job you are doing.

The CHAIRMAN. Thank you, Senator Thurmond.

Senator Schumer.

Senator SCHUMER. Thank you very much, Mr. Chairman, and thank you for having these timely hearings. I think it is so good that we are having hearings before any proposals are before us on an important issue. I am new to this issue and am glad we are also trying to make it a good, strong judiciary issue.

So I have some questions, I guess. My first question deals with my experience with privacy issues and with other kinds of issues in the House. And one of you mentioned this, but no one focuses on it. Usually, when government is importuned to act, it is because there are bad actors. There are not the IBM's or the AOL's, but others who do things that horrify people. And sure as we are sitting here, there are going to be bad actors who do something. They will sell private medical records that they get hold of or something like that.

What do any of you suggest we do, just say, well, you know, relying on the marketplace? That won't work. These are market-driven decisions. Self-regulation? That doesn't work. By definition, a bad actor doesn't submit to self or industry regulation. How do we deal with bad actors, and if we don't deal with them, isn't it likely that they will just grow and grow and grow, and actually hurt you folks who are trying to do—I respected the statements that everyone has done here because you are trying to do the best work.

So that, to me, is the fundamental question here, not the 95 percent of those involved who would find a balance. Left to your own devices, you will find a balance between freedom of speech and privacy rights, but there are some who won't.

Yes, the gentleman from IBM.

Mr. WLADAWSKY-BERGER. Senator Schumer, first of all, as my colleague from AOL said before, the Internet is a medium, and it is a wonderful, mysterious, very flexible medium. But what is happening more and more is that the technology is now disappearing into the woodwork and enabling lots of applications.

Now, for a lot of bad things that would happen on the Internet, there are probably already laws to handle those bad things because people are doing things over the Internet that have been done for many, many years. And so one thing for sure is to have a good understanding whether existing practices protect that, and if so, apply those protections. And then when they don't, then one can look at incremental changes to the protection. So I would say that is point No. 1.

Senator SCHUMER. If I might, I agree with you, and certainly in an ideal world you could apply the—the Internet basically just speeds information up.

Mr. WLADAWSKY-BERGER. Right.

Senator SCHUMER. It doesn't change the transaction of information. However, because things are so quick, there are detection problems; there are problems that are different than non-Internet problems, in actuality.

Go ahead.

Mr. WLADAWSKY-BERGER. I agree totally with you. It is not identical; it is an extension. I mean, the reason it has exploded in the marketplace, and the reason there is so much activity is that it is such a phenomenal extension. But for lots of problems, there are probably already recourses. That is the only point we should understand.

I think point No. 2 is I would say that massive education is needed so that consumers, businesses, everybody knows sort of the rules of the road. This is what is expected, this is what you should do, this is what shouldn't happen. And we are all pretty comfortable that the more education there is, the better things will get. Maybe it is a little bit naive, but we have seen already——

Senator SCHUMER. The more education, the better the good people can be and the worse the bad people can be.

Mr. WLADAWSKY-BERGER. I realize that, but lots of things can happen also if consumers realize this is what you should expect from Web sites you deal with. So it is not just that there won't be bad Web sites, it is that the invisible hand in the sense of they lose all their customers will take care of that.

And then when that doesn't work, then we are not against legislation. We are not against the Government acting. We are saying let's not do it on a broad basis; let's do it for highly targeted problems when we find them. And protection of minors, protection of very sensitive information like medical records, might be in that category where we do need legislation. And when we find those highly targeted categories, by all means we should take action.

Senator SCHUMER. Yes, Mr. Berman.

Mr. BERMAN. There is a lot of truth in what he says. We have a very weak privacy regime for data in this country. We talk about privacy, but it is pretty thin in terms of legislation. There is no medical privacy. There is higher protection for video records than

for medical records, and higher for video records than financial records.

So there is a whole set of sectors where we have stopped doing any work or haven't been able to break the logjam between the different sides which need to be resolved because that information is moving on the Internet. So there are specific problems that need to be resolved.

I think the difficult issue, and I think it is worth working on, is what are the remedies for violations in the commercial transaction world. When I talk about medical records and the big database, I understand someone ought to go to jail for that. There is a problem when you get down to when L.L. Bean takes—and forget their name—without my permission, gives my name and my address to REA, and they did it intentionally. There is a harm there, but what is it, and what do we impose on REA?

If we don't figure that out and make it clear and specific and proportional, a lot of little companies aren't going to go into business. IBM can figure that out and go to court, but the vagueness, due process, and First Amendment issues that are raised by privacy remedies have not been addressed.

Senator SCHUMER. I agree with you. I mean, we have had this in credit cards in the Banking Committee and we still haven't come to a good solution. But in reference to what Mr. Wladawsky said, you are right, we haven't come to this, but the Internet—I mean, hospital records; 20 years ago, the damage that would occur to your privacy would be maybe if someone who had access to those records gave them to a friend and somehow you heard about it. When it happens, the damage is limited and it doesn't happen that often.

With the Internet, the chances of those records being spread to everyone in the world is much greater. That is the quantum difference here, which is a serious difference, and that is why we are having these hearings and we never had hearings on these privacy issues before.

Yes, Mr. Sheridan.

Mr. SHERIDAN. I think the context is what we are talking about. The Internet is in many places simply replacing certain processes, and there is no real protection for medical information bureaus for what they do. And they have been selling our information, and it may be even worse than not having it in the Internet because at least on the Internet, I am on that network. Before, there was a network between the insurance company who is checking my application for health insurance or life insurance and I have no idea what is going on.

So what I am trying to say is this is in the context of the Internet is an attractive target for it, but it is actually a much broader problem than that.

Senator SCHUMER. It is, but the Internet is bringing it to a head. That is the bottom line here, and I still think we are going to have to figure out, whether we do anything or not, some way to deal with bad actors. It may be as simple as what Mr. Berman said, increased penalties for those who do. Maybe there needs to be a greater prophylactic measure. I don't know. I am just getting into this. All I can tell you is I think the problem is not going to go away. I think it is going to get worse because the bad actors have

more clout and more ability to do things, and we have to deal with it.

I just had one other question. Did you want to say something, Ms. Borsecnik?

Ms. BORSECNIK. The only other comment I would add to that is they are also more highly visible and more exposed in this medium, which is a good thing for everyone. I think an enormous amount of attention is paid when these things happen. So I think rather than them proliferating like mushrooms in the dark somewhere, they will be further exposed in our industry because it is so open.

Senator SCHUMER. Yes, and you will have a greater—I mean, there is a privacy issue and there is an accuracy issue, and the accuracy issue will—as I think Mr. Sheridan mentioned, that will be better because it will be out in the open, as you say. But the privacy issue is still one that hasn't been dealt with.

Mr. SHERIDAN. It is like Mr. Berman is saying that there is a very fine line between our other freedoms.

Mr. BERMAN. One point. We have worked on privacy issues before, particularly the law enforcement and privacy balance.

Senator SCHUMER. Yes.

Mr. BERMAN. And I said at the start of my testimony that Senator Leahy's effort to look at the Fourth Amendment issues on the Net are incredibly important because these companies are creating new kinds of data that make the Monica Lewinsky book purchase subpoena a piece of cake; I mean, just incredibly sensitive data being put away from your home and on the Internet. And we have got to figure out the standards of access for that for government agencies as against——

Senator SCHUMER. This is one other point that I would like to make, a separate point, as somebody who is not as proficient as my children on this, but I am sort of learning. So I usually late at night read a national publication on the Internet, and I was wondering why they did it because I don't have to buy it the next day. And, you know, they got smart and last week they changed the whole system where you can only read parts of it now.

But they also made me register and they just said, you know, they wanted my name and all that, but they wanted my phone number. Well, I didn't want to give them my phone number to get this, only because I wanted to make sure that they wouldn't give it to 30 people who would keep interrupting us at dinner.

And I, who is probably middle-level proficient, but assuming from everything you say that everyone is going to be using this service, so I will probably move to a higher-level of proficiency over the next few years—I couldn't find out what they were going to use my phone number for. I punched around, I went to "Help," I did everything I could. I could not find out why they wanted to use my phone number, so I didn't register.

So there is a long way even on the things—forgetting the bad actor for a minute, this related to what you said, Ms. Borsecnik, that those of us who are not as proficient as you have very sort of elementary questions that for a semi-literate person in this area is very hard to figure out the answers to.

Ms. BORSECNIK. And you didn't register and they lost a customer, so they are going to realize that pretty quickly that they are losing people.

Senator SCHUMER. But they have no idea why I didn't register.

Ms. BORSECNIK. Well, it will become obvious.

Mr. BERMAN. Yes, they will figure it out.

Senator SCHUMER. They will?

Ms. BORSECNIK. Oh, yes.

The CHAIRMAN. Or you can type in 11111.

Senator SCHUMER. Well, you know what? I thought about that. [Laughter.]

I thought of doing 1234567, and then I said, well, you know, maybe I better check if I am violating some kind of rule or something like that. [Laughter.]

The CHAIRMAN. Well, that is why I said 11111, because some poor slob could have that 1234567.

Senator SCHUMER. That is true, that is true. Good point. You know what, Mr. Chairman? This is a pretty good political opportunity.

Mr. BERMAN. It might have been his phone number.

Senator SCHUMER. I would never do that to my Chairman, for whom I have tremendous esteem and respect.

Mr. SHERIDAN. We are actually developing a product that will, if you choose to as your own personal policy, fill that in with random information that will appear correct, and it will be different every time.

Senator SCHUMER. Ms. Borsecnik wasn't so happy with that idea. [Laughter.]

Well, Mr. Sheridan, if you want to establish a branch office in New York that has 80 or 90 people to do that, I would be all for it.

Mr. SHERIDAN. We have quite a few people in New York.

Senator SCHUMER. Anyway, please.

Ms. BORSECNIK. My point was my view is that companies shouldn't be collecting information that is not necessary to run their business, or they should make it very obvious what is optional, what is not optional, and how you can exercise choice about how that information is used.

Senator SCHUMER. By the way, I wouldn't have even minded if this company wanted my phone number to solicit me for them. But I was worried they would sell it to somebody or to a lot of somebodys.

Ms. BORSECNIK. Right.

Senator SCHUMER. Thank you, Mr. Chairman.

The CHAIRMAN. You are welcome.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman. My concerns, in a sense, parallel Senator Schumer's. I, like him, am somewhat a newcomer to the Internet. I am the proud possessor of a new Think Pad which I enjoy very much.

Mr. WLADAWSKY-BERGER. Thank you.

Senator FEINSTEIN. You are welcome. [Laughter.]

However, I have watched this privacy issue two-fold. The first has to do with the giving out of personal financial and medical in-

formation, some of it the most intimate details. And I have noticed then people begin to bring it in the public arena, and slowly the industry begins to respond by some form of self-regulation.

I also have concerns on the other element of privacy and, of course, that is the pedophile looking for a victim. That is the drug cartel using highly encrypted computer technology to conspire to move tons of cocaine into this country, and that is the terrorist, as we found in the Philippines, using the privacy that encryption provides to conspire to blow up airliners.

I am as heartened by anything, frankly, as Mr. Berman's comments this morning that the industry is beginning to realize that it has to be more vigilant with respect to self-regulation. I mean, I know of no excessive legislation being proposed anywhere, certainly in this body, with respect to regulation. I do, however, think the jury is out with respect to self-regulation. And there are many of us with respect to children and crime that are really watching very carefully.

I, for example, will look to see where the youngsters from the incident yesterday in Denver got the information to put together the 30 explosive devices that they put at that school and whether it came, in fact, from the Terrorist Handbook, something that I have been trying to get off the Internet for 5 years now. It gets passed in the Senate and it gets deleted in the conference. So I have a little bit of frustration when I see somebody advertising, if you want to learn how to build a bomb that is bigger than the one at Oklahoma City, just read this.

There was a cartoon in a California newspaper that showed a mother talking on the phone to a friend who said, I am so pleased with Johnny, he is learning so much from the Internet. And there is Johnny over at his computer stringing together sticks of dynamite. And so I only say that because it is a problem out there and children have blown themselves up, and I have enough testimony to know that that is an accurate statement.

The question is really what we do about the abuses. Now, I am not talking about the companies, but the real abuses. And I would be interested, Mr. Berman, if you would be willing to expand a little bit on your comments in this direction.

Mr. BERMAN. Well, it depends on the case we are dealing with. Certainly, in the real abuses, the pedophile, the people collecting information from children, and even the marketer who, under false pretenses, collects information and sells it, to my detriment, there needs to be a set of penalties, both civil and criminal, that make it clear that that is unacceptable behavior.

Senator FEINSTEIN. Is your organization willing to work in this direction?

Mr. BERMAN. Absolutely.

Senator FEINSTEIN. I would like to work with you.

Mr. BERMAN. As you know, we have had a debate about where to draw these lines, and I just got appointed by Senator Daschle, for good or for evil, to the COPA commission to again look at the issue of indecent communications on the Internet and what to do about that. I want to try and find solutions to keep that information away from children, but to try and do it consistent with this technology and the First Amendment.

Two times I have said to the Congress I agree with your goals, but it is not going to work legally, so why don't we work a little more closely together to try and fine-tune this? And I think that solutions are possible, both in the First Amendment area and the privacy area, but it requires everyone taking a deep breath both on the privacy front and the law enforcement front, and even on the pornography front, and saying these are hard questions. We know it when we see it, but someone's Spam is someone else's First Amendment leaflet. How do we sit down and craft remedies? I am glad to work on that. It is just not a fast train.

Senator FEINSTEIN. It is very interesting. As a newcomer to this, I am so amazed by the power of it and the speed with which the technology is improving. I mean, just to keep up, I have had to buy two new computers in 4 years. Things change so fast.

And I think none of us want to impinge on the First Amendment. On the other hand, one of the things I have been very concerned about is drugs coming into this country, and cocaine literally coming in by the ton and the inability to do anything about it. And we are told constantly that intelligence intercepts are way down because the telephone isn't being used anymore. Therefore, they can't get court orders to tap a phone because the phone isn't being used. But another vehicle is being used, and that, of course, is the computer. So how we get at this to prevent these kinds of major conspiracies also I think is something I would like very much to work on. I don't know the answers.

Mr. BERMAN. Well, my experience has been that whether it is passing the Foreign Intelligence Surveillance Act or the Electronics Communications Act—that tells how long I have been around here—in all of these statutes, where law enforcement issues and privacy issues have been on the table, it ultimately requires some consensus and tradeoffs on both sides.

Law enforcement may need "A" and clarification of its authority to do something, but at the same time Congress needs to be looking at the need for adjustments on the privacy side so that there is an increase in privacy as well as law enforcement and national security. Every time you have been able to find that kind of balance so that everyone has something to gain from it, you have a chance to craft meaningful legislation.

Senator FEINSTEIN. I am really heartened to hear that. Your testimony today, for me, was a major step forward from what I have been hearing for the last 6 years, and I just want to thank you and commend you for it.

If anybody has any other comments to make on that, I would like to hear them, but I would like to ask Ms. Borsecnik something about your written statement just very quickly. You implied that AOL doesn't read private online communications, but you said that you carefully monitor your children's chat rooms and message boards.

Ms. BORSECNIK. Right.

Senator FEINSTEIN. How do you do this?

Ms. BORSECNIK. Well, there is a difference between private and public communications online. Private communications are e-mail and instant messages. They are one-to-one. They are sent in privacy. There are also public areas online. Chat rooms are public

areas and message board areas are public areas. That is very clear to users.

In our policies, we set forth our policy, as you reiterated, on private communication. We also say that we hold our members to a certain conduct standard online, particularly in the areas that are targeted at kids and teens, and that we monitor what goes on in that area. Typically, the kind of transgressions we act against are your pretty typical profanity or threatening other members, the things that go on just sort of on a normal basis among——

Senator FEINSTEIN. Do you send this to all members?

Ms. BORSECNIK. Members review that all——

Senator FEINSTEIN. You have never sent it to me. I am a member.

Ms. BORSECNIK. When you first registered with America Online and we talked to you about what we call our terms of service, that information is included in that. And you are required as part of the registration process to click a button that said I have read this and I agree to the terms of service.

Senator FEINSTEIN. I never did.

Ms. BORSECNIK. It is also available online in a number of places where you can find it easily. I can send you a link or whatever. But, clearly, ensuring that people are aware of what those policies are is important for a variety of reasons, not the least of which is ensuring an enjoyable experience online, not only a safe and privacy-secure one, but an enjoyable experience for the rest of our customers.

So we have rules of the road just like any other community, and in an online environment it is a little harder to convey what those rules are because people are anonymous. You wouldn't tend to stand up in a public forum and be profane. In an online environment where there is anonymity, we take extra efforts to explain to people what those community guidelines are. And that is even more true in the public arenas, as you mention, but we do have strict policies against private arenas, which are e-mail, for example.

Senator FEINSTEIN. Could you send me some of that information that everybody gets? I would love to see it.

The CHAIRMAN. I wouldn't mind receiving it, also.

Ms. BORSECNIK. I will send it to all of you.

Senator FEINSTEIN. Thank you.

The CHAIRMAN. That would be great.

Senator FEINSTEIN. Thank you very much. Let me just ask one other question about children. I think we all agree that children present certain distinctive privacy issues due to their greater vulnerability. So I think it follows that children should be treated differently by Web sites operators and online service providers. The tricky issue, I think, is how do you determine when one actually is a child and when one isn't a child.

I would be interested in hearing from each of you as to how a Web site operator or an online service provider could go about determining whether an individual is really a child or not.

Ms. BORSECNIK. I will answer that first. It is a little easier for AOL because to use AOL, you become a member. You need to use a credit card to become a member, and so it is not typical for chil-

dren to have credit cards. We make it very clear in the registration process that to register as a member, you need to have a credit card and you need to be 18 years or older.

Then, furthermore, we very aggressively encourage parents with children in the household to set up separate screen names for those children and designate them in certain age categories so that we can block certain functionality or areas on the Internet or our service from those kids.

Senator FEINSTEIN. Could you send me that information as well?

Ms. BORSECNIK. Yes, that will all be included and it is all explained in that document.

Senator FEINSTEIN. Thanks. I appreciate it. Thank you. Anybody else on that? Yes, sir.

Mr. FISCHBACH. We are in the video game business and it is a real, ever-present question to us as to how we determine who a child is because it is certainly easy for them to say that they are not a child, or they just come onto the site and look around or they drop their e-mail address.

The guidelines that we have chosen to follow are pretty clear in terms of what we use that information for, so we don't ask for his address. We don't ask for financial data, we don't ask for medical records, we don't ask for credit cards. The most that we ask for is an e-mail address at that juncture. What we are trying to determine as an organization and also as a company is how much further should we go in order to determine whether he or she is or is not a child.

Should we ask them to give us her parent's address or e-mail address? Should we ask for a telephone number for them? The more information that we attempt to extract, the more information we then have available to us and we are not interested in that information. We are not interested in somebody coming back. So it is really a question, and we as an industry organization are trying to look at how to best handle that situation. There is not a 100 percent answer.

One of the ways that we just attempted to look at it was just to limit the amount of information because kids will come online and play games. They will ask for information about our next products. They will want to know if we have got a bug—if there is a bug in a game, and all software has bugs, if there is a fix for it. If I can't get from level 12 to level 13, how do I do it? And they will come and ask that information and we will pass information back to them. So it is a difficult issue and I don't know how we do it. There is not a 100-percent pure answer for it.

Senator FEINSTEIN. Please, anybody that wants to comment.

Mr. BODOFF. I was going to say the answer is easy to say we require parental verification before you can collect information from a child. What is difficult is determining what is parental verification, and we are really looking forward to some new technology approaches and new ideas. What we are using now is basically what the Federal Trade Commission has referenced, and we use as examples credit cards or e-mail information from the parents before you can actually accept personally identifiable information from the child.

But we all know children are creative, and that is a challenge. And we all, I think, in the business community are going to be looking for different ways of trying to improve upon that, but we definitely have a criteria that you cannot collect information from a child under the age of 13 without parental verification.

Senator FEINSTEIN. Could I ask a question? Why was 13 set as the age?

Mr. BODOFF. We are modeling after the Online Privacy Act, the Children's Online Privacy Act, the Online Privacy Alliance. It is the feeling that I think—and I am not an expert in the children's area, but below 13 children do not have enough cognitive sense to be able to make the right decision when somebody is asking them to solicit information and how that is being used. And above that age, children start having that capability and there is a higher confidence level with that.

Senator FEINSTEIN. Anybody else on that?

[No response.]

Senator FEINSTEIN. I think that is it. Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Feinstein.

Let me just finish with one or two. Mr. Fischbach, I know you did not come here to testify about the nature of the products you sell and make available over your Web site, but many in America are trying to come to grips with the terrible tragedy that occurred yesterday in Colorado, and really in Salt Lake City as well, but especially in Colorado, where two dysfunctional young men murdered as many as 14 fellow students and a teacher, and then turned the guns on themselves.

I predict that we will learn over the coming days that those Trenchcoat Mafia boys were obsessed with death and killing, and that much of what fueled their obsession came from the Internet and other media sources. In my opinion, our young people are exposed to too much violence and killing in our popular culture. You turn on a television set and you have got murder happening all the time. You flip through any number of the channels and it is hard to find a show where somebody is not being killed. You listen to today's music and its obsession with death and distress, groups like Marilyn Manson, which apparently these Trenchcoat Mafia members idolized.

Another source for violence and death, of course, is video games. And I am not meaning to pick on you, but I would like to have you answer this because I think it is important for all people in this industry to realize that we watch stuff like this. Take, for example, Acclaim's "Shadow Man." Now, I would note that Acclaim has many games on the Web site that are totally all right and that are not violent.

This morning, however, we went to your Web site and took a look at some of the other games your company offers and stumbled across "Shadow Man." Now, here is how your game information Web page reads, "A killer is coming walking between worlds, trailing death from live side to dead side. A dead man is coming, scull in one hand, gun in the other, a voodoo mask in his chest and lines of power in his back. A possessed man is coming, stalking killers in tenements and deserts, subways and swamps, spirit world and

real world. Shadow Man is coming, voodoo slave and hero, hitman and dead man. Sometimes, it takes a killer to stop a killer. Uniquely terrifying third-person adventure. Enter the dark world of Mike Leroy, hitman, dead man, Shadow Man. Blow your enemies away body and soul. Go in armed with voodoo power and gunpowder. Pack weapons like the 50-magnum Desert Eagle, the Violator, the Flambeau, the Calabash, and many more. Unravel the dark mysteries or die trying. More than just another blood-drenched shootout."

Now, could you tell us how many people access "Shadow Man" on your Web site daily? Do you have that kind of information.

Mr. FISCHBACH. We can provide that to the committee if the committee was interested in that.

The CHAIRMAN. OK.

Mr. FISCHBACH. I can say we are equally as appalled with what happened in the schoolyard as you and everybody else.

The CHAIRMAN. No, I don't mean to blame you for that, but I just cite this because it seems to me this is one of the illustrations of what is happening in our society.

Mr. FISCHBACH. I think, in part, there are lots of factors that take place in what goes through young people's minds—what kinds of homes they come from, how they are dependent on other people, whether their families are really dysfunctional.

We also have a very open gun environment in our society, where anybody can go buy weapons and anybody can buy ammunition to do what they please with. Yet, we don't sometimes point at those issues and say maybe that is part of the problem as well.

There have been lots of studies that have been done with respect to violence and video games or violence and television or violence and motion pictures, most of which conclude that that is not the cause, especially of people like these young men here, as to why they become dysfunctional in our own society and do acts that we are all appalled by. So it is very, very difficult, and it is an issue that we all are confronted with. I mean, Kosovo is on the front page, as well as this other one, and we deal in a society that is very violence-oriented.

The products are a fantasy, and the products are a fantasy no different than a book or a film or a television show. And both of us know that you can't go from life side to dead side, which is the fantasy to begin with. And the game is really an adventure game that is very suspenseful as you go through. It is based on a comic book, not unlike many of the films or many of the books that have already been turned into films or video games. It is part of our culture.

The CHAIRMAN. Well, as you can see, you are making a pretty good case that we have got a culture that seems to foster this. I remember the Tupac Shakur matters and how he was calling for killing police people and a lot of other things like that.

For our information, it would be interesting for me to know how many people access "Shadow Man" on your Web site daily, whether or not you know how many of them are children, and how many video-depicted killings they engage in in a typical round and, in addition, if you could tell me whether you share my view that there is a collective dumbing-down of young people's attitudes toward vi-

olence. And I am not blaming you or the Internet solely. There is no question that the Internet has its bad side.

Mr. FISCHBACH. With respect to "Shadow Man" or the sports games that sit on our Web site at this point in time, that is mere publicity and I don't believe there is a downloadable function from that, except they can take a visual if they want to take a visual from it. But there is no game-play that is up on our Web site that we have released at this juncture. So all it is is a statement about what the game contains, and I think some pictures about what the game contains.

The CHAIRMAN. OK.

Mr. FISCHBACH. And in terms of the number of people or whether they are children or not, we don't ask them. So you can access our Web site without asking our permission, whether you are a child or not.

The CHAIRMAN. But even if you did, you may not be able to know. These kids are very clever.

Mr. FISCHBACH. The game also carries an "M" rating on it, so the game is identified for a mature audience. It is not identified for children.

The CHAIRMAN. I see. You know, I held a hearing on Internet sales of alcohol and I figured that would be an interesting hearing. You can't believe the fur that has been stirred up because of that, and you can't believe the arguments on all sides of that issue. I mean, it was really amazing how complex and difficult it was, as certainly exists with this.

I didn't mean to pick on you, but I thought I would bring that out because we all know that there are problems with the Internet. We all know there are things that are wrong about the Internet. We all know there are many, many wonderful things that are right about it, too, and I would like to accentuate the "rights" and see what we can do to alleviate the "wrongs."

Senator FEINSTEIN. Mr. Chairman, would you let me ask just one quick question?

The CHAIRMAN. Sure.

Senator FEINSTEIN. Would you agree that this adds to the culture of violence that is being promoted in the United States?

Mr. FISCHBACH. I can't answer that question because—I personally don't think so. I think the culture that we live in is reflective of lots of other environments, and I think with respect to the culture that we live in today with respect to how we use guns and ammunition, which I am highly opposed to, I think we are wrong. I think there is no legislation that deals with guns that is really effective.

When we talk about what should exist and what shouldn't exist, and you say we are going to point it toward a film or we are going to point it toward a book and we are going to say, OK, that is the answer, I think that is a real simple approach. I mean, it is like a check mark, and if you looked at some of the other things that exist in our society, because we have access to all kinds of information, just not what sits on our Web site, but what sits in public records and what sits in libraries, what sits in films, it all has an influence.

So you either take a paint brush and eradicate it all or you deal with it as a society through education. But there are elements in our society that can be dealt with, such as weapons, because there is no reason why anybody, especially a 17-year-old kid, should walk around with a gun or be able to go buy ammunition.

Senator FEINSTEIN. Of course, I happen to agree with that.

Mr. FISCHBACH. Thank you.

Senator FEINSTEIN. And I have tried very hard, which is not an easy thing to do around here.

The CHAIRMAN. I give her an opportunity every chance I get. [Laughter.]

Let me tell you, we already have a law that forbids selling of guns to minors. It isn't perhaps working, and there is no easy solution because we have people all over this country who value their right to keep and bear arms. We have those who abuse that right. But again, as Senator Feinstein has said, there is a culture here that no one individual, no one business, no one entity is to blame for all of it. But I think we all need to work on it and that is the only reason I raised that.

Let me just say one last thing here. As I noted in my opening statement today, much of the discussion about possible solutions revolve around two exclusive models, either Government regulation by the FTC, the FCC, or some other regulatory body, or sole industry self-regulation. Mr. Berman, you have indicated we ought to go as far as we can on self-regulation, but there is going to have to be some aspect of regulation.

As many argue against the merits of either one of these solutions, I think it would be productive to explore whether another solution possibly exists; for example, examining quasi-governmental self-regulatory models that have been successful in other industries. That is what we need to do, it seems to me. I think it is important to not establish rigid rules in this area, and instead have a flexible system in place that can respond quickly to changing consumer preferences and new technologies, like digitalme, perhaps, designed to give consumers more control over personal identifiable information.

I don't know whether we have enough information about what it is exactly that consumers expect in terms of privacy protection, or even how this is effected. A flexible system would best be accomplished through self-regulation by members of the electronic community who are aware of consumer demands and expectations, it seems to me.

I would like to get your views on whether a model similar to the one in the securities industry could be useful to address privacy on the Internet, a model where the basic codes of conduct are established by the industry with limited Government oversight to provide for a level of consumer confidence in the process.

Now, if you believe it could be a useful model, I would kind of like to conclude this hearing by asking you to work with me over the coming days and weeks to develop a reasonable but limited legislative proposal that might help to solve some of the problems that all of you recognize exist in ways that don't stifle the industry and don't stifle innovation and creativity.

I think that is a pretty big assignment, but that is one reason why we are holding this hearing to see if we can find some methodologies or some ways of solving these problems that will protect society, and yet make sure that we continue to go forward as the leaders in the world in this area.

So why don't I start with you, Mr. Wladawsky-Berger, and then maybe you, Mr. Sheridan; you, Borsecnik; and Messrs. Berman, Bodoff and Fischbach. You don't all have to comment, but if you would like to.

Mr. WLADAWSKY-BERGER. Mr. Chairman, clearly, what should unite us here is the fact that we want the potential of the networked economy for the Nation to be fulfilled and all the positive things to happen and eliminate the negatives. And what that really means is that it is all very pragmatic. We are after a common objective, and if there are things that are highly targeted that can help us better achieve that objective within a self-regulatory mechanism, we would be very happy to work with you and investigate what those things might be.

As I said in my testimony, and as we have discussed through the hearing, the only concern, or the main concern we have is, because things are moving so fast in such a complicated area, that we have regulations that will not work and that will make it harder for the objectives to be accomplished.

However, if we can find highly selected areas where we can do some good, and we talked about protection of minors as one; protection of very sensitive information like medical records might be another that can help start setting the right mechanisms. And as we learn more, we learn more of what else to do. We will be very happy to work with you and see what makes sense.

The CHAIRMAN. Well, as you know, one reason we held the Microsoft hearings was not just to try and resolve some problems that exist, but basically, I am a firm believer that unless we attack these problems now, you are going to have an over-regulatory nature, and that would be very detrimental to the Internet and to our future and to our future governance of these innovative and creative matters.

So I think those hearings have proven to be the beginning of something very important. And I don't wish my friends at Microsoft any harm. I think the world of what they have been able to do, but there were some things that needed to be corrected and I think they are going to be corrected in the end.

And it is important that we move in these directions because the last thing on Earth I want is an over-regulation of the Internet. But at least I have seen from the shaking of heads that all of you kind of indicate that there needs to be something here. And I don't want these wonderful, genius Members of Congress to just come up with it themselves. My experience has been that they may have a genius of sorts, but without an awful lot of help, we could really screw up the Internet, and I don't want to see that happen.

Mr. Sheridan, do you have any comments about that?

Mr. SHERIDAN. Yes. We would, Mr. Chairman, be more than happy to work with you on a middle way, something in between.

The CHAIRMAN. Put some time into it because, you know, you have been right in the middle of all this. And, you know, my expe-

rience with the Internet creators is that they just love to burrow in and solve the engineering problems, but they are not really concerned about the legal problems or the statutory problems.

Mr. SHERIDAN. Social problems.

The CHAIRMAN. Social problems, yes, and I think you are going to have to be because the last thing on Earth you want is to have us come in here with a heavy hand.

Mr. SHERIDAN. We agree.

The CHAIRMAN. That is where it is headed, I can tell you, and I am trying to stop it with everything I can. And I think in the end, Microsoft may not thank me, but the fact of the matter is I think they will be better off in the end as well.

Mr. SHERIDAN. We would be very happy to explore new models and look at what has worked, how can it be simple and flexible around a model that, as you were saying, is a hybrid. We would be glad to participate in that, and we would also like to see what laws could be better enforced, say, around medical issues and things that are——

The CHAIRMAN. Right. Well, see, that is another big issue. I am very, very concerned. People say, well, we should be able to disclose people with emotional illness so they can't get guns. Well, there are a myriad set of problems there, everything from litigation and malpractice to—I mean, it is mind-boggling. And I would like to do that. I mean, I would like to be able to find some way that we could prevent that without destroying people's lives or their privacy, and it is pretty hard to do. But you folks, I think, may have the keys to do that.

Ms. Borsecnik, as you know, I have tremendous respect for AOL and I have been very impressed with you here today, but do you have any comments on this?

Ms. BORSECNIK. Well, I think the issue you just brought up—we keep using the example in the health care industry—conveys the concern of the one-size-fits-all issue. And I think Senator Kohl's suggestion of a commission that looks further into all the various sectors that are affected by privacy——

The CHAIRMAN. A commission that might be supervised by the Government, you are saying?

Ms. BORSECNIK. Yes, because I think, as you said at the beginning, we are in the first inning on this discussion and the debate because of the myriad of complicated issues and industries involved. And we encourage that kind of discourse because only through that will we be able to focus on a solution that provides a standard that is acceptable, but is workable across a variety of businesses and a variety of consumer concerns.

The CHAIRMAN. I am going to come to you last, Mr. Berman, since you have been the one who has been so crass as to recommend this process.

Mr. Bodoff.

Mr. BODOFF. The only thing I would add—and I have heard from two of our sponsors, AOL and IBM at the table here with me, and that is probably reflective of the other companies who have been instrumental in building our program—is that whatever happens, we don't do anything that discourages companies from joining self-regulatory activities.

We have a great challenge in front of us now. We have got to get out and educate businesses and we have got to get businesses to make a commitment. And we are only open a month and we have some very aggressive plans, and I think if we were talking at the end of the year, we would see some very interesting results, the danger being in any activity that holds out something else and lots of companies who may be moving toward a self-regulatory approach right now hold off because they are waiting for something else. They are fearful of something else or something else is happening. So I would only ask that that be given consideration in any action that takes place.

The CHAIRMAN. Thank you. Mr. Fischbach.

Mr. FISCHBACH. Well, I think that as we continue moving forward, I put down in my notes paint brush as opposed to a small, thin brush, because each particular sector is going to have its own particular issues. And if we are too broad in whatever we attempt to do from a congressional standpoint, I think that the answer will probably harm us as oppose to help us with respect to the economics that can come from the Internet, plus the fact that it is really a worldwide issue. It is not just a local issue as to what takes place in the United States because of the access of information and where you can set your sites up.

We would be happy to participate in some sort of a body which would study and make recommendations in terms of how to handle this, the suggestion of a commission to work on what kinds of legislation or rules should be passed. The problem, I think, is we know where we are today; we are not sure where we are going to be in 3 to 4 years from today and what changes will take place in technology and how we will move information back and forth. Some of it we can anticipate, but it will change the way that all of us do business and it will change the way that we access information.

The CHAIRMAN. Thank you. Now, Mr. Berman, we will let you sum up for everybody.

Mr. BERMAN. I think that we are all committed to the growth and dynamism of the Internet, and we want to make sure that it has the right fundamental law, and that commerce goes on and privacy is protected, and the free flow of information. And I think that the right approach is somewhere between these extremes, which is to really hone in and work together to bring the industry and the privacy advocates and policy experts together and try and work through these issues, to find the flexible—it doesn't have to be one-size-fits-all, but to work toward resolving some very hard issues of how to get fair information practices out on the Net. So we are pleased to work with you and the committee. We have done it before and we will do it again.

The CHAIRMAN. Well, let me just challenge all of you to really live up to that because I would like to have the very best ideas you have. This committee has been doing some pretty good things in this area, in my opinion, and we are capable of doing many more good things, but we have got to have the right advice and the right counsel to be able to do them right.

You know, there are so many problems, but I cite this problem. Since yesterday's murders in the Colorado school, I have been hit all over the place by people saying, well, we have got to have dis-

closure, at least from a weapons standpoint, of people's mental illness. The mental illness societies are going berserk over this because they know that once that starts, they are going to be discriminated against if it isn't handled absolutely right.

Can it be handled absolutely right? Can we do something that really is a privacy type of thing that will work so that people are not discriminated against who have had an emotional disturbance at one time in their lives? If the truth is known, probably every one of us has suffered emotionally from time to time. Whether it rises to the dignity of having to have special professional help or not is another matter.

But it is a big problem because everybody comes up with these broad-brush—you know, we have got to stop all weapons, or we have got to do this, or we have got to make sure nobody who has an emotional illness or even emotional distress has access to weapons. Well, that is just one very small, little aspect of this whole thing. You get into all the others, credit cards right on through, and it is almost mind-boggling.

And you are kind of suggesting a private sector commission, set up maybe by the industry, that is supervised by maybe some sort of governmental supervision or regulation. My problem with Government is, once regulation starts, it becomes a stifling aspect to what really is, in the minds of many, one of, if not the most important set of opportunities in America's history, and one of, if not the most important industry in America right now, because from this industry almost everything we do in the future is going to be connected.

So we would really like to have some ideas here before some people want to ram through some idiotic, stupid approach toward this that creates another Internet IRS, which goes from a few hundred pages to 6,000 pages overnight. I just don't want to see that happen.

This has been a very good hearing. We are very grateful to each and every one of you for coming because each of you has expressed different aspects of this set of problems, and I think it has been a very, very good panel. So thank you so much.

With that, we will adjourn until further notice.

[Whereupon, at 12:51 p.m., the committee was adjourned.]

APPENDIX

ADDITIONAL SUBMISSIONS FOR THE RECORD

April 23, 1999

The Honorable Orrin Hatch
Chairman, Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Dianne Feinstein
331 Hart Senate Office Building
Washington, DC 21510

The Honorable Patrick Leahy
Ranking Member,
Senate Judiciary Committee
152 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Hatch, Senator Leahy and Senator Feinstein:

On behalf of America Online, I want to thank you and the entire Judiciary Committee for inviting Katherine Borsecnik, AOL's Senior Vice President for Strategic Businesses, to appear before the Committee this week to discuss online privacy issues. I hope you found the testimony and discussion to be informative and helpful.

In response to Senator Feinstein's specific request at the hearing, I am forwarding to you additional information about some of AOL's member policies. Specifically, I have enclosed a copy of AOL's Terms of Service (which includes the AOL Member Agreement, the AOL Community Guidelines, and the AOL Privacy Policy), as well as a copy of AOL's guidelines for using "parental controls" to protect children online. Each document includes a cover page that illustrates how the material appears online to an AOL subscriber, followed by the complete text of the document itself.

Here is a brief explanation of each of these documents:

- The *AOL Terms of Service (TOS)* is a complete statement of AOL's commitments to our members, as well as an explanation of our members'

Law and Public Affairs Group • Suite 400 • 1101 Connecticut Avenue, NW • Washington, DC 20036-4303
202/530-7878 • FAX 202/530-7879
http://www.aol.com/

rights and responsibilities when using the AOL service. The TOS is comprised of the following three documents:

* The *AOL Member Agreement* is a legal document that details the rights and obligations of each AOL member. An individual cannot become an AOL Member until he or she has accepted the terms of the Member Agreement. The Member agreement includes a description of billing policies and the procedures for termination or cancellation of a member's AOL account.

* The *AOL Community Guidelines* set forth the rules and standards for proper online content and conduct within the AOL service.

* The *AOL Privacy Policy* outlines our core principles for protecting the personal privacy of our members, and explains how we handle personal information online and what choices our members have regarding the use of that information.

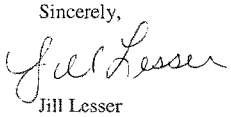
- *AOL's Parental Controls*: This is an excerpt of the material that is provided to our members to explain some of the ways in which parents can take steps to protect their kids online, including a guide to setting up special accounts for kids that restrict what they see and whom they may interact with online.

As Ms. Borsecnik explained during the hearing, this information is provided to our members when they first sign up for AOL, and is easily accessible at any subsequent time through links from related areas or by typing Keyword: "TOS," "Privacy," or "Parental Controls."

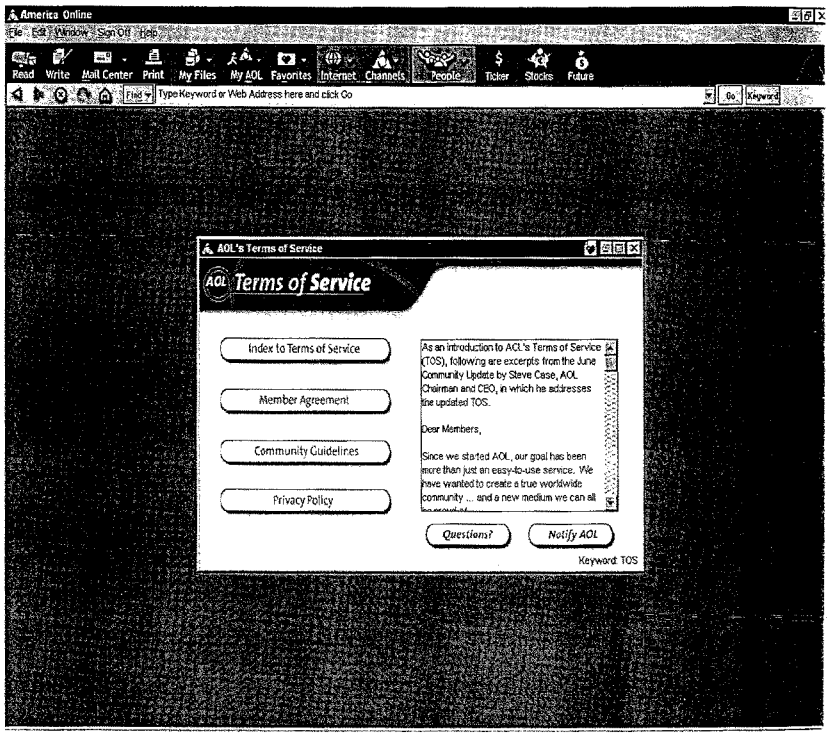
We want you to know, especially in light of the appalling events that recently unfolded in Littleton, Colorado, that AOL is committed to guaranteeing our members the highest standards for privacy and safety online. We will continue to look for ways to improve our own service in this regard, and will work with our industry colleagues to address issues relating to online security and help make the Internet safe for all users.

Please let us know if we can provide any additional information to you. We appreciate your interest in these important issues, and look forward to continuing to work with you.

Sincerely,



Jill Lesser
Vice President, Domestic Public Policy
America Online, Inc.


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Ticker Stocks Future
Find Type Keyword or Web Address here and click Go
Go Keyword
AOL's Terms of Service
AOL Terms of Service
Index to Terms of Service
Member Agreement
Community Guidelines
Privacy Policy
As an introduction to AOL's Terms of Service (TOS), following are excerpts from the June Community Update by Steve Case, AOL Chairman and CEO, in which he addresses the updated TOS.
Dear Members,
Since we started AOL, our goal has been more than just an easy-to-use service. We have wanted to create a true worldwide community ... and a new medium we can all
Questions?
Notify AOL
Keyword: TOS

As an introduction to AOL's Terms of Service (TOS), following are excerpts from the June Community Update by Steve Case, AOL Chairman and CEO, in which he addresses the updated TOS.

Dear Members,

Since we started AOL, our goal has been more than just an easy-to-use service. We have wanted to create a true worldwide community ... and a new medium we can all be proud of.

The essence of community, however, is more than the technological capability to bring people together online ... it is developing the trust that will keep them there. And the key to building a medium to be proud of is building our members' confidence in the safety of our medium.

The foundation of our relationship with our members is our Terms of Service or TOS. The TOS contains our commitments to you, as well as your rights and responsibilities as an AOL member. Because the TOS is so important to our members' experience, we decided to update it to make it as clear, complete and easy to use as our service itself.

In short, we are making two commitments to you. First, we are determined to help lead our industry by setting high standards for our policies and practices. Second, we are determined to do everything possible to live up to them. And let me assure you that if any failures occur or new issues arise, we will deal with these situations quickly and forthrightly -- and keep you fully informed about what we are doing and why.

The new TOS will go into effect on July 15. We hope it will foster the kind of trust that will allow you to feel secure and to take full advantage of the medium's promise and potential.

This Terms of Service is divided into three parts -- the Member Agreement, the Community Guidelines and the Privacy Policy -- all written in what we hope you will find to be a straightforward, "plain English" style. I urge you to read all three policies. We've also redesigned the TOS online area (Keyword: TOS) to make it easier for you to access all topics, find answers to your questions, and send us your comments.

Despite this new format and style, there is little change in the way we do business or how we expect our members to conduct themselves online. Here's a brief summary of each of the three elements of TOS.

** The Member Agreement contains the basic legal terms of an AOL Membership. It covers things like our cancellation policy, the responsibilities of the master account holder and our procedures relating to billing and surcharges. Despite the legal nature of the topics, we've done our best to write the Member Agreement in a clear, concise way. And we've tried to make it easy for you to ask questions.

** Our Community Guidelines explain the common-sense principles for how all members should behave online to ensure everybody's right to enjoy this medium, such as observing all laws; showing basic manners; using good judgment; and not sending unsolicited bulk e-mail or "spam."

** Our Privacy Policy sets out the principles that we believe are necessary to protect your privacy as an AOL member. As I mentioned, we recognize that respecting your privacy online is one of our most important jobs. So we have rewritten our privacy policy to make it as clear as possible and made it a separate section of the TOS.

Our new privacy policy, which you can read anytime you're online by going to Keyword: Privacy, is based on eight principles that help you understand exactly how we use your personal information and what choices you have. To review these principles right now, click on the Privacy Policy button to the left.

At the end of the privacy policy, we have also provided a checklist of ten steps you can take to safeguard your privacy and protect the integrity of your computer and AOL account. We urge you to print out this checklist and post it near your computer for you and your family.

In addition, we have redesigned our Marketing Preferences area to make it easier for you to understand and make choices about how your data may be used by us for marketing. You can get to the Marketing Preferences area by going to Keyword: Choice or Keyword: Marketing Preferences. It also includes an Interest Profile you may fill out to let us know the topics about which you'd like to be informed.

We have also made it easier for our members to ask questions about our TOS through the Questions button in this new TOS area, as well as on the privacy policy at Keyword: Privacy Questions. In the future, when it becomes necessary for us to update one of these three policies in important ways, we will make sure you receive the opportunity to review these changes before they occur.

We recognize that kids deserve a special level of protection, which is why we've developed new, separate policies for children and young teens. The basis of our kids' privacy policy is Parental Permission First -- we and our partners require the permission of a parent before we will collect any personal information in areas designed specially for children 12 and under. Our kids' policies also require that advertising in kids' areas be clearly marked and the content on AOL and on Web sites linked from kids' areas be appropriate for children.

Finally, as we all know, policies are only as good as the people who enforce them. I want to explain to you the steps that we are taking to put our updated TOS comprehensively and effectively into action -- particularly our privacy policy.

* We have distributed and will make sure all of our employees fully review the updated TOS, including attending a training session to explain how it applies to their jobs.

* Every AOL employee -- including all Member Services representatives -- is required to sign electronically a document stating that he or she has read and will comply with the Privacy Policy. Employees who violate our Privacy Policy are subject to disciplinary action, up to and including termination.

* Only authorized AOL employees are permitted to have access to your personal information and that access is limited by need and by strict guidelines for how they may use it.

* We have become a sponsor of TRUSTe, the independent, nonprofit organization that certifies adherence to posted privacy policies on Web sites. We will have the TRUSTe seal on AOL.COM, our Website.

We are committed to delivering to you the most enriching and fulfilling online experience available anywhere. These updated, easy-to-understand policies and practices underscore that commitment. I hope you'll take the time to see for yourself ... and let us know what you think.

Warm regards,

Steve Case

The AOL Terms of Service is provided below. You may review, print, save or search on any section of the Member Agreement, Community Guidelines or Privacy Policy (the three documents that make up AOL's Terms of Service), by clicking on the blue, underlined text.

You may also review, print, save or search the Member Agreement, Community Guidelines or Privacy Policy in their entirety.

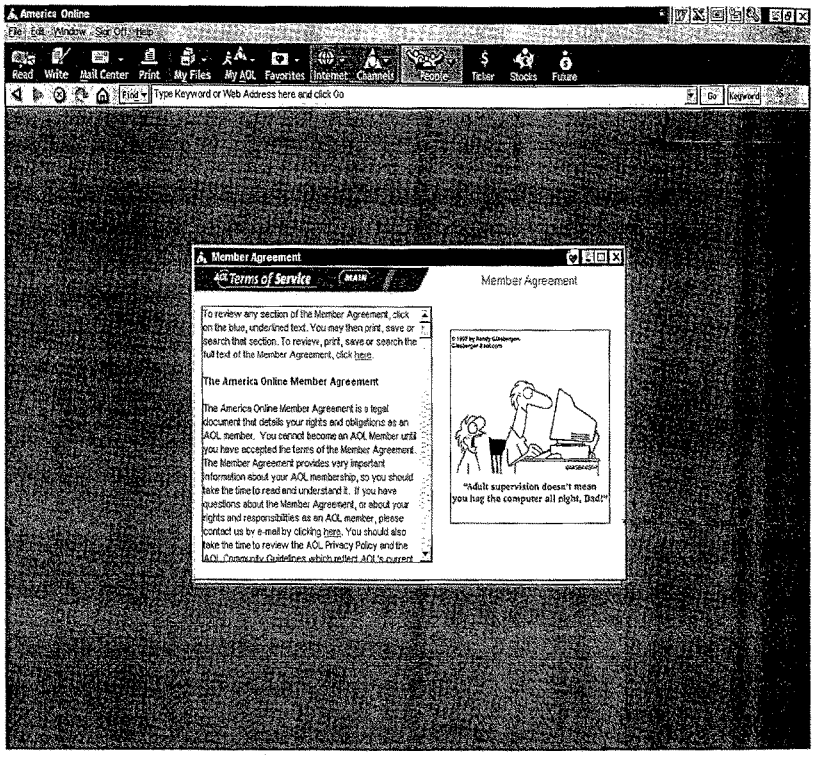
AOL Terms of Service

The America Online Member Agreement
1. The Basics of Your AOL Membership
2. Charges and Billing
3. Online Conduct and Content
4. AOL Software Licenses
5. Warranty
6. Indemnification
7. Termination and Cancellation
8. Law and Legal Notices

AOL Community Guidelines
1. Appropriate Online Content
2. Proper Online Conduct
3. Illegal Behavior
4. Unsolicited E-mail
5. Protection of Copyrights and Trademarks
6. Content and Behavior on the Internet
7. International Online Areas
8. Getting Help: Online Resources

AOL Privacy Policy
1. Confidentiality of your private communications.
2. Privacy regarding where you go on AOL and the World Wide Web.
3. Privacy regarding your personal contact information, and how to update or correct it.
4. Privacy of your online purchases.
5. Your choices regarding use of your personal contact information.
6. Privacy and safety in areas designated for children.
7. Safeguards for your personal information.
8. Notice about our privacy policy and updates to it.

Ten Tips to Help you Protect Your Privacy and Security Online


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Ticker Stocks Future
Find Type Keyword or Web Address here and click Go
Go Keyword
Member Agreement
Terms of Service
MAIN
Member Agreement
To review any section of the Member Agreement, click on the blue, underlined text. You may then print, save or search that section. To review, print, save or search the full text of the Member Agreement, click here.
The America Online Member Agreement
The America Online Member Agreement is a legal document that details your rights and obligations as an AOL member. You cannot become an AOL Member until you have accepted the terms of the Member Agreement. The Member Agreement provides very important information about your AOL membership, so you should take the time to read and understand it. If you have questions about the Member Agreement, or about your rights and responsibilities as an AOL member, please contact us by e-mail by clicking here. You should also take the time to review the AOL Privacy Policy and the AOL Community Guidelines which reflect AOL's current
"Adult supervision doesn't mean you hog the computer all night, Dad!"

The America Online Member Agreement is a legal document that details your rights and obligations as an AOL member. You cannot become an AOL Member until you have accepted the terms of the Member Agreement. The Member Agreement provides very important information about your AOL membership, so you should take the time to read and understand it. If you have questions about the Member Agreement, or about your rights and responsibilities as an AOL member, please contact us by e-mail by clicking here. You should also take the time to review the AOL Privacy Policy and the AOL Community Guidelines which reflect AOL's current policies. The Internet and online world is changing rapidly and as technology and AOL's business continue to evolve, these policies may have to be updated or revised. Since these Privacy Policies and Community Guidelines may change, you should check Keyword: TOS for the most current versions.

For the same reasons, it may be necessary for AOL to update or revise certain provisions of the Member Agreement. By joining AOL and accepting the Member Agreement you agree that AOL may change the terms of this Member Agreement. **If AOL makes material changes or revisions to the Member Agreement, we will provide notice to you thirty days in advance. If you don't agree to the changes proposed by AOL, or to any of the terms in this Member Agreement, your only remedy is to cancel your AOL membership.**

1. THE BASICS OF YOUR AOL MEMBERSHIP

This Agreement is your entire agreement with AOL and governs your use of the AOL Internet online service. There may be additional terms and conditions if you use affiliate services like our international areas, other AOL services or products such as AOL Instant Messenger(TM) service or third-party software and/or services. To access the AOL service you must accept the terms of this Agreement and comply with the AOL Community Guidelines. To be an AOL member, you must be at least 18 years old. If you are not yet eighteen years old, you may still use AOL, but only if the account was created and registered by your parent or guardian. Because we give out free trial offers, we reserve the right to limit you to just one free trial.

When you accept this Agreement and complete the AOL registration process, you become the "master account" holder, and AOL provides you with a limited, non-exclusive license for no more than the term of your membership to use the screen name you select for your "master account." AOL also allows you to have up to four additional "sub-accounts" or screen names of your choice. Your screen name is your online identity. You may not use a screen name that is used by someone else, and your screen name cannot be vulgar, or be used in any way that violates the other parts of the Member Agreement or the Community Guidelines.

As the master account holder, you are responsible for all activity on your account and on any of the sub-accounts, and violations or warning accrued by the sub-account can lead to termination of the master account. If warnings or violations are received by sub-accounts, the master account will also receive notification. You may also receive important notices about your membership from time to time that may not be provided to the sub-accounts, so it is important for you to regularly check your master account mailbox. Because you are responsible for all use of your account, you should supervise the use of your account by others. This is especially important when children are using the service; children are safer online and get more out of the experience with adult supervision. It is important that you not reveal your password to other users and AOL will never ask you for your password. You agree not to reveal your password to other users and you agree to indemnify and hold AOL harmless for any improper or illegal use of your account. This includes illegal or improper use by someone to whom you have given permission to use your account. Your account is at risk if you let someone use it inappropriately. If your membership is terminated for violating this Agreement or the Community Guidelines, AOL's express permission will be necessary before you are allowed to use AOL again.

2. CHARGES, BILLING AND THE FREE TRIAL

AOL reserves the right to change our fees or billing methods at any time and AOL will provide notice of any such change at least thirty days in advance in the same manner described above for changes to the Member Agreement. AOL also has the right to collect applicable taxes and impose premium surcharges for some areas of the service and these surcharges may apply even during your free trial. The answers to many common billing questions can be found by going to Keyword: Help, then selecting Accounts & Billing, going to Keyword: Billing, or by contacting an AOL customer service representative at 1-800-827-6364. If you don't like the changes in fees or billing methods, you may cancel your membership at any time, but AOL will not refund any remaining portion of the monthly fee when you cancel your membership. **If you have joined AOL as a trial member, you should understand that your free trial time must be used within one month of your initial sign-on and to avoid being charged a membership fee, you must cancel your account before the end of that first month.**

As the master account holder, you are responsible for all charges incurred, including applicable taxes and purchases made by you or anyone you allow to use your account or sub-accounts, including your children, other

members of your family or friends. This means that, unless your account or credit card information is obtained unlawfully or fraudulently by someone other than those authorized to use your account or sub-account, you will be responsible for all usage and purchases under your account or sub-accounts.

There may be extra charges to access certain premium content on AOL. AOL will provide notice of any extra charge before you enter the premium area. You are responsible for any charges for premium content incurred using your account (including sub-accounts) and these charges apply even during the free trial. AOL's Parental Controls allow you to prevent sub-accounts from accessing premium or surcharged content. For more information go to Keyword: Parental Controls. Some Web sites charge separate fees, which are not included in the cost of your AOL membership. AOL provides access to a large number of third-party vendors, who provide content, goods and or services on the AOL service or the Internet. Any separate charges or obligations you incur in your dealings with these third-parties are your responsibility and are not part of the fee charged for your AOL membership.

Most members pay by credit card. For most billing plans we will be charging your designated card every month, but some charges may accumulate on your account before they are charged to your card. If you don't have a credit card, you can authorize AOL to make electronic fund transfers from your checking account. There is an additional surcharge for this payment option and you should go to Keyword: Billing and read about AOL's Billing Methods for more information. By selecting this billing option and providing AOL with your debit/checking account information, you authorize AOL to debit your checking account for charges incurred using AOL. Every time you use AOL, you re-affirm that AOL is authorized to charge your credit card or withdraw funds via electronic transfer from your checking account, depending on which payment method you have selected. You also agree to authorize AOL to charge purchases you make online to the credit card you supplied to AOL when you joined or to debit your checking account if you selected that option during the registration process.

We expect you to pay your account balance on time. We will give you 30 days from the date on your account statement to pay your bill. AOL will assess an additional 1.5% (or the highest amount allowed by law, whichever is lower) per month late charge if your payment is more than 30 days past due. That amount is also due immediately. You are responsible and liable for any fees, including attorney and collection fees, that AOL may incur in its efforts to collect any remaining balances from you. You also agree that you will be billed for and will pay any outstanding balances if you cancel your membership or are terminated. You should let us know about any billing problems or discrepancies within 90 days after they first appear on your account statement. If you do not bring them to AOL's attention within 90 days, you agree that you waive your right to dispute such problems or discrepancies.

AOL has an extensive network of access phone numbers throughout the country, but it is still possible that the nearest AOL access number might be a long distance or toll call from your location. Any telephone charges incurred connecting to AOL are your responsibility. Since these charges are your responsibility, you should contact your local telephone company if you have a question about whether an AOL access number is a long distance or toll call from your location. AOL also provides several surcharged 800 or 888 access phone numbers (for the current surcharge rate go to Keyword: Access). If you choose to use these surcharged numbers to access AOL, you agree to pay the currently applicable surcharge to AOL. If you have other questions about access phone numbers, you should consult Keyword: Access. It is important to note that you can incur long distance or toll charges or surcharges for 800 or 888 access even during your free trial.

3. ONLINE CONDUCT AND CONTENT

Content

By content, we mean the text, software, communications, images, sounds and other information provided online. Most content on the AOL service is provided by AOL, our members, our affiliates, or independent content providers under license. In general, AOL does not pre-screen content available on the AOL service. AOL does not assume any responsibility or liability for content that is provided by others. AOL does reserve the right to remove content that, in AOL's judgment, does not meet its standards or does not comply with AOL's current Community Guidelines, but AOL is not responsible for any failure or delay in removing such material. Keep in mind that AOL is not responsible for content available on the Internet, although we reserve the right to block access to any Internet area containing illegal or other harmful content or otherwise being used for purposes that are unlawful or injurious to AOL or its members.

One of the most exciting aspects of this medium is that individual members have the ability to create their own content and voice their own opinions. AOL encourages Members to participate and express their views -- after all, that is what makes your experience interactive. But it is important to remember that there are rules and standards that you must abide by as an AOL Member. These rules and standards are described in the AOL Community Guidelines. As an AOL Member, you agree to follow the AOL Community Guidelines and you acknowledge that AOL has the right to enforce them in its sole discretion. This means

that if you, or anyone using your account, violate the AOL Community Guidelines, AOL may take action against your account. This can range from the issuance of a warning about a violation to the termination of your account. You understand AOL is not required to provide notice prior to terminating your account for violating these rules and standards, but it may choose to do so. Additionally, as an AOL member, you may have access to other AOL branded services, such as AOL Instant Messenger(TM) service, that are available to both AOL members and to other Internet users. When using these AOL branded services, your conduct remains subject to this Member Agreement; however, non-AOL members who use these services are not subject to this Member Agreement and as a result you understand that these other users may not be governed by the same rules or standards. Because of the changing nature of the Internet and Online Services, the Community Guidelines may change at any time. You can always find the most current version of the AOL Community Guidelines at Keyword: TOS.

Unsolicited Bulk E-mail
Your AOL membership allows you to send and receive e-mail to and from other AOL members and users of the Internet. This does not mean that you may use AOL to send unsolicited bulk e-mail or junk e-mail. Information about unsolicited bulk e-mail can be found at Keyword: Junk Mail. Your AOL membership and your authorization to use the AOL e-mail service do not allow you to send unsolicited bulk e-mail or to cause unsolicited bulk e-mail to be sent by someone else. **You may not use the Member Directory or any other area of AOL to harvest or collect information, including screen names, about AOL members, and the use of such information for the purpose of sending unsolicited bulk e-mail is strictly prohibited.** Any violation of these provisions can subject your AOL account to immediate termination and further legal action. If you have received junk e-mail and want to report it, simply use the **Forward** button on the e-mail screen and send the e-mail to screen name **TOS Spam**. AOL also reserves the right to take any and all legal and technical remedies to prevent unsolicited bulk e-mail from entering, utilizing or remaining within the AOL Network.

Proprietary Rights
Much of the content available on our service is owned by others, and is protected by copyrights, trademarks, and other intellectual property rights. It is very easy to copy things in cyberspace, but just because it is easy doesn't mean it is acceptable or legal. Any content that you upload or download while using the service must be authorized; this means you must have the legal right to upload or download the content. You must not copy, transmit, modify, distribute, show in public or in private or create any derivative works from any of the content you find on AOL, unless you have the legal right to. Making unauthorized copies of any content found on AOL can lead to the termination of your AOL account and may even subject you to further legal action beyond the termination of your membership. Similarly, other content owners may take criminal or civil action against you. In that event, you agree to hold harmless AOL and its subsidiaries, affiliates, related companies, employees, officers, directors and agents.

Bear in mind that some areas of AOL are "public," like message boards, forums, or the Member Directory, and other members will have access to your posted material and might copy, modify or distribute it. By submitting or posting content there, you are representing that you are the owner of such material or have authorization to distribute it. Once you post content on AOL, you expressly grant AOL the complete right to use, reproduce, modify, distribute, etc. the content in any form, anywhere.

4. AOL SOFTWARE LICENSES

AOL provides you with a limited license to use our software, which you agree to use in accordance with these rules. You may not sub-license, or charge others to use or access, our software without first obtaining written permission from us. We will occasionally provide automatic upgrades to improve your online experience, and we employ virus-screening technology to assist in the protection of our network and our members. We reserve the right to log off accounts that are inactive for an extended period of time and we prohibit the use of tools that defeat AOL's automatic log-off feature.

AOL grants to you a non-exclusive, limited license to use AOL software to connect to AOL from authorized locations in accordance with this agreement. This license is subject to the restriction that, except where expressly permitted by law, you may not translate, reverse-engineer or reverse-compile or decompile, disassemble or make derivative works from AOL software. You may not modify AOL software or use it in any way not expressly authorized by this Agreement. You understand that AOL's introduction of various technologies may not be consistent across all platforms and that the performance and some features offered by AOL may vary depending on your computer and other equipment.

5. WARRANTY

MEMBER EXPRESSLY AGREES THAT THE USE OF AOL, AOL SOFTWARE, AND THE INTERNET IS AT MEMBER'S SOLE RISK. AOL, AOL SOFTWARE, AOL PRODUCTS, THIRD-PARTY VIRUS CHECKING TECHNOLOGY AND THE INTERNET ARE PROVIDED "AS IS" AND "AS AVAILABLE" FOR YOUR USE, WITHOUT WARRANTIES OF ANY KIND, EITHER

EXPRESS OR IMPLIED, UNLESS SUCH WARRANTIES ARE LEGALLY INCAPABLE OF EXCLUSION. AOL PROVIDES THE AOL SERVICE ON A COMMERCIALLY REASONABLE BASIS AND DOES NOT GUARANTEE THAT MEMBERS WILL BE ABLE TO ACCESS OR USE THE SERVICE AT TIMES OR LOCATIONS OF THEIR CHOOSING, OR THAT AOL WILL HAVE ADEQUATE CAPACITY FOR THE SERVICE AS A WHOLE OR IN ANY SPECIFIC GEOGRAPHIC AREA. AOL'S ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY WITH RESPECT TO THE USE OF ANY SOFTWARE PROVIDED OR USED BY AOL SHALL BE THE REPLACEMENT OF ANY AOL SOFTWARE FOUND TO BE DEFECTIVE. YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY OTHER DISPUTE WITH AOL IS THE CANCELLATION OF YOUR ACCOUNT AS DETAILED BELOW IN SECTION 7. IN NO CASE SHALL AOL BE LIABLE FOR CONSEQUENTIAL DAMAGES ARISING FROM YOUR USE OF AOL, THE INTERNET OR FOR ANY OTHER CLAIM RELATED IN ANY WAY TO YOUR MEMBERSHIP WITH AOL. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR THE LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, AOL'S LIABILITY SHALL BE LIMITED TO THE EXTENT PERMITTED BY LAW. AOL DOES NOT ENDORSE, WARRANT OR GUARANTEE ANY PRODUCT OR SERVICE OFFERED THROUGH AOL AND WILL NOT BE A PARTY TO OR IN ANY WAY BE RESPONSIBLE FOR MONITORING ANY TRANSACTION BETWEEN YOU AND THIRD-PARTY PROVIDERS OF PRODUCTS OR SERVICES.

6. INDEMNIFICATION

Upon a request by AOL, you agree to defend, indemnify and hold harmless AOL and its affiliated subsidiaries, employees, contractors, officers, directors, telecommunications providers and content providers from all liabilities, claims and expenses, including attorneys fees, that arise from a breach of this Member Agreement for which you are responsible or from the use of AOL or the Internet, or in connection with your transmission of any Content on AOL. AOL reserves the right, at its own expense, to assume the exclusive defense and control of any matter otherwise subject to indemnification by a Member. In that event, the member shall have no further obligation to provide indemnification for AOL in that matter.

7. TERMINATION AND CANCELLATION

Either you or AOL may terminate or cancel your membership at any time. You understand and agree that the cancellation of your account is your sole right and remedy with respect to any dispute with AOL. This includes, but is not limited to, any dispute related to, or arising out of: (1) any term of this Agreement or AOL's enforcement or application of this Agreement; (2) any policy or practice of AOL, including AOL's Community Guidelines and the AOL Privacy Policy, or AOL's enforcement or application of these policies; (3) the content available through AOL or the Internet or any change in content provided through AOL; (4) your ability to access and/or use AOL; or (5) the amount or type of fees, surcharges, applicable taxes, billing methods, or any change to the fees, applicable taxes, surcharges or billing methods.

You can cancel your membership by delivering notice to AOL's Customer Service Department at 1-888-265-8008, by sending your cancellation request via US Mail to: AOL, PO Box 1600, Ogden UT 84401, or by fax at 1-801-622-7969. **Cancellation will take effect within 72 hours of receipt of your request, and AOL will send you written confirmation. If you cancel near the end of your billing period and are inadvertently charged for the next month's fee contact AOL at the toll free number above to have the charges reversed.** AOL reserves the right to collect fees, surcharges or costs incurred before you cancel your AOL membership. In addition, you are responsible for any charges incurred to third-party vendors or content providers prior to your cancellation.

In the event that your account is terminated or canceled, no refund, including any membership fees, will be granted; no online time or other credits (e.g., points in an online game) will be credited to you or can be converted to cash or other form of reimbursement. Active AOL Members may not allow former Members or other agents whose memberships have been terminated to use their accounts. Any delinquent or unpaid accounts or accounts with unresolved issues with the Community Action department or other AOL departments must be concluded before you may re-register with AOL, Inc.

8. LAW AND LEGAL NOTICES

The Member Agreement represents your entire agreement with AOL. You agree that this Member Agreement is not intended to confer and does not confer any rights or remedies upon any person other than the parties to this Agreement. You also understand and agree that the AOL Community Guidelines and the AOL Privacy Policy, including AOL's enforcement of those policies, are not intended to confer, and do not confer, any rights or remedies upon any person. If any part of this Agreement is held invalid or unenforceable, that portion shall be construed in a manner consistent with applicable law to reflect, as nearly as possible, the original intentions of the parties, and the remaining portions shall remain in full force and effect. The laws of the Commonwealth of Virginia, excluding its conflicts-of-law rules, govern this Agreement and your membership. As noted above, member conduct may be subject to other local, state, national, and international laws. You expressly agree that exclusive

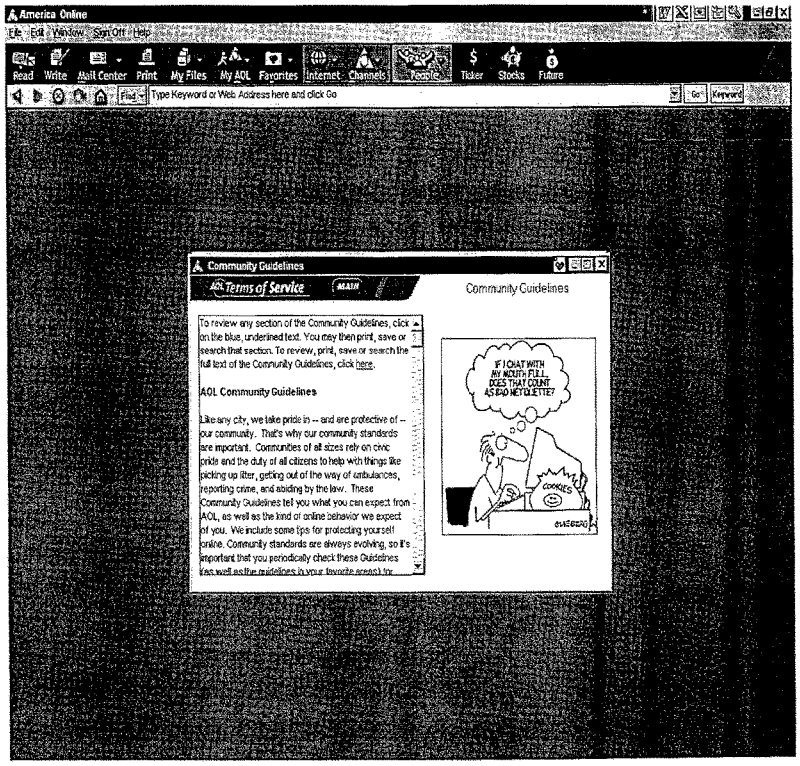
jurisdiction for any claim or dispute with AOL or relating in any way to your membership or your use of AOL resides in the courts of Virginia and you further agree and expressly consent to the exercise of personal jurisdiction in the courts of Virginia in connection with any such dispute including any claim involving AOL or its affiliates, subsidiaries, employees, contractors, officers, directors, telecommunication providers and content providers.

You agree to abide by U.S. and other applicable export control laws and not to transfer, by electronic transmission or otherwise, any content or software subject to restrictions under such laws to a national destination prohibited under such laws, without first obtaining, and then complying with, any requisite government authorization. You further agree not to upload to AOL any data or software that cannot be exported without prior written government authorization, including, but not limited to, certain types of encryption software. This assurance and commitment shall survive termination of this agreement. Control laws currently prohibit the export of any browser with 128-bit encryption, including Internet Explorer, available through AOL. Control laws also prohibit nationals of Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria from gaining access to certain content on AOL.

Information for California Residents:
Under California Civil Code Section 1789.3, California Members are entitled to the following specific consumer rights information:

Pricing Information. Current rates for using AOL may be obtained by calling 1-800-827-6364. AOL, Inc. reserves the right to change fees, surcharges, monthly membership fees or to institute new fees at any time upon thirty (30) days prior notice, as provided for in the Member Agreement at Section 2.

Complaints. The Complaint Assistance Unit of the Division of Consumer Services of the California Department of Consumer Affairs may be contacted in writing at 1020 N. Street, #501, Sacramento, CA 95814, or by telephone at 1-916-445-1254.


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Ticker Stocks Future
Find Type Keyword or Web Address here and click Go
Go Keyword
Community Guidelines
AOL Terms of Service
MAIN
Community Guidelines
To review any section of the Community Guidelines, click on the blue, underlined text. You may then print, save or search that section. To review, print, save or search the full text of the Community Guidelines, click here.
AOL Community Guidelines
Like any city, we take pride in -- and are protective of -- our community. That's why our community standards are important. Communities of all sizes rely on civic pride and the duty of all citizens to help with things like picking up litter, getting out of the way of ambulances, reporting crime, and abiding by the law. These Community Guidelines tell you what you can expect from AOL, as well as the kind of online behavior we expect of you. We include some tips for protecting yourself online. Community standards are always evolving, so it's important that you periodically check these Guidelines (as well as the guidelines in your favorite areas) for
IF I CHAT WITH MY MOUTH FULL, DOES THAT COUNT AS BAD NETQUETTE?
COOKIES

Like any city, we take pride in – and are protective of -- our community. That's why our community standards are important. Communities of all sizes rely on civic pride and the duty of all citizens to help with things like picking up litter, getting out of the way of ambulances, reporting crime, and abiding by the law. These Community Guidelines tell you what you can expect from AOL, as well as the kind of online behavior we expect of you. We include some tips for protecting yourself online. Community standards are always evolving, so it's important that you periodically check these Guidelines (as well as the guidelines in your favorite areas) for updates, new information, or additional safety tips. It's all part of taking pride in and protecting the AOL community. Thanks for doing your part.

Here are the basics (read further for more detail):

* Appropriate online content.
* Proper online conduct.
* Illegal behavior.
* Unsolicited e-mail.
* Protection of copyrights and trademarks.
* Content and behavior on the Internet.
* International online areas.
* Getting help: Online resources.

Appropriate online content.

By content, we mean the information, software, communications, images, sounds, and all the material and information you see online. It is provided by AOL, our international joint ventures, our members, or under license by our content partners. We do not pre-screen content generally, but our content partners are expected to ensure that their content on the service reflects our community standards. We reserve the right to remove content that does not meet those standards. Neither AOL nor its partners assume any liability if the content is not removed. Bear in mind that we can do this only on the AOL service: we cannot do it on the Internet outside AOL. (see Content and Behavior on the Internet).

Members like you also generate content in chat rooms, message boards, Web pages, etc. It is essential that this kind of content also reflects our community standards, and we may remove it if, in our best judgment, it does not meet those standards. When we do, you may receive a warning about the violation of AOL's standards if your account (any of the screen names) was responsible for putting the objectionable content online. If it's a serious offense or you've violated our rules before, we may terminate your account.

AOL applies the same standards to its own and its partners' content that it applies to member content. Remember that community standards vary from community to community. Some chat rooms may use stronger language than others. Obviously, some online areas may deal with more adult-oriented topics, such as sexual dysfunction, rape, or infidelity, and we offer our members Parental Controls so that you may ensure that kids who use your account can't see that mature content (see Getting Help: Online Resources). In most places on AOL, vulgar language or sexually explicit conduct are no more appropriate online than they would be at Thanksgiving dinner. So while the guidelines may vary a bit depending on the online area you're in, in general, these guidelines apply:

Language: Mild expletives and non-sexual anatomical references are allowed, but strong vulgar language, crude or explicit sexual references, hate speech, etc. are not. If you see it, report it at Keyword: Notify AOL.

Nudity: Photos containing revealing attire or limited nudity in a scientific or artistic context is okay in some places (not all). Partial or full frontal nudity is not okay. If you see it, report it at Keyword: Notify AOL.

Sex/Sensuality: There is a difference between affection and vulgarity. There is also a difference between a discussion of the health or emotional aspects of sex using appropriate language, and more crude conversations about sex. The former is acceptable, the latter is not. For example, in a discussion about forms of cancer, the words "breast" or "testicular" would be acceptable, but slang versions of those words would not be acceptable anywhere.

Violence and drug abuse: Graphic images of humans being killed, such as in news accounts, may be acceptable in some areas, but blood and gore, gratuitous violence, etc., are not acceptable. Discussions about coping with drug abuse in health areas are okay, but discussions about or depictions of illegal drug abuse that imply it is acceptable are not.

Please bear in mind that these are only guidelines; there is always a "gray area." Use your best judgment. Ask yourself if this

is something that you would say in a room full of people you never met, or in the workplace. However, AOL makes the final determination about whether content is objectionable or not.

With all the content posted on AOL every day by our members, we can't possibly monitor all of it, and we do not attempt to do so. Therefore, you might occasionally encounter something you don't want to see. You can ignore it, but we prefer you report it using the Keyword: Notify AOL. Good judgment is important, especially when you encounter the opinions of others. AOL doesn't endorse or oppose opinions expressed by our members, but we do sometimes take issue with the manner in which the opinion is expressed. Hate speech is never allowed.

Proper online conduct.

Online conduct should be guided by common sense and basic etiquette. You will be considered in violation of the Terms of Service if you (or others using your account) do any of the following:

* Post, transmit, promote, or distribute content that is illegal.

* Harass, threaten, embarrass, or do anything else to another member that is unwanted. This means: don't say bad things about them, don't keep sending them unwanted Instant Message(TM) notes, don't attack their race, heritage, etc. If you disagree with someone, respond to the subject, not the person.

* Transmit or facilitate distribution of content that is harmful, abusive, racially or ethnically offensive, vulgar, sexually explicit, or in a reasonable person's view, objectionable. Community standards may vary, but there is no place on the service where hate speech is tolerated.

* Disrupt the flow of chat in chat rooms with vulgar language, abusiveness, hitting the return key repeatedly or inputting large images so the screen goes by too fast to read, etc. This is online vandalism, and it ruins the experience for others.

* Pretend to be anyone whom you are not. You may not impersonate another member (including celebrities), an AOL employee, or a Community Leader.

* Attempt to get a password, other account information, or other private information from a member. Because a member's account is that person's online existence and persona, it is sacrosanct. Remember: AOL employees will NEVER ask for your password. Don't give your password or billing information out to anyone.

Obey the rules wherever you are. This includes the rules of other interactive services, AOL area guidelines, state, local, federal laws, or foreign or international law where appropriate. Ignorance of the law is no excuse. "Netiquette" is used all over the Internet. Whether you are on AOL or using other Internet functions, it's important to be polite. Many newsgroups, Web communities, and the like have their own community guidelines or standards, and you should consult them before interacting.

Remember that new AOL features or technologies are always subject to the Terms of Service.

Illegal behavior.

The laws that apply in the offline world must be obeyed online as well. We have zero tolerance for illegal behavior on the service. We terminate accounts and cooperate with law enforcement on such matters.

In addition to providing you with an easy way to report illegal activity, we or our partners may in some instances monitor public areas. Our Community Leaders are there to help you and to help us maintain community standards. We do not monitor private areas, such as private chat rooms, Instant Message(TM) conversations, or e-mail. Regardless of the area, AOL may be used only for lawful purposes. Just because we may not be monitoring the area you're in at that point in time doesn't mean we won't uphold our standards. In addition, AOL reserves the right to treat as public any private chat room whose directory or room name is published or becomes generally known or available.

Unsolicited e-mail.

* Unsolicited bulk e-mail is strictly prohibited.

* Chain letters and pyramid schemes are not allowed. Many such things are illegal. Even the ones that aren't illegal are annoying to most people and tie up online resources, so we don't allow them.

* You may place advertisements only in areas designated for that purpose. Unsolicited advertising is not allowed. This includes the sending of bulk e-mail. You must have permission from AOL and/or the person to whom you are sending the ad.

* You may not use the Member Directory or any other area of AOL to harvest or collect information, including screen names, about AOL members, and the use of such information for the purpose of sending unsolicited bulk e-mail is strictly prohibited. This includes collection of names on a member Web page. You must adhere to AOL's Privacy Policy.

* You can regulate the mail you receive by going to Keyword: Mail Controls.

Mail Controls allow you to:
* Block or allow all e-mail
* Block or allow e-mail from specific addresses or from the Internet
* Block domains (the sources of the mail)
* Block file attachments to e-mail

Protection of copyrights and trademarks.

Some content is owned by others and is protected by copyrights, trademarks, and other intellectual property rights. It's very easy to copy things in cyberspace, but just because it's easy doesn't mean it's acceptable or lawful. Unauthorized copying of software is illegal, and you can be subject to criminal penalties beyond the termination of your membership. We take this seriously. Similarly, other content owners may take criminal or civil action against you. All the content you transmit must either be your own or must be transmitted with express authorization for distribution on AOL.

Bear in mind that some areas of AOL are "public," like message boards, forums, or the Member Directory, and other members will have access to your posted material and might copy, modify or distribute it. By submitting content in these public areas, you grant to AOL the complete right to use, reproduce, modify, distribute, etc. the content in any part, anywhere.

Content and behavior on the Internet.

AOL provides you with access to the Internet, which is different from AOL. E-mail to or from non-AOL members, newsgroups, FTP, the World Wide Web, etc. are outside of the boundaries of AOL. However, as an AOL member you are required to follow our TOS no matter where you are on the Internet. If another ISP or Internet organization reports you to us, we will take appropriate action against your account the same as we would if you had committed a violation on the AOL service.

AOL offers Web site publishing capability to encourage you to participate in a variety of online communities on AOL. We regard such communities as part of the AOL service, and we will enforce our community guidelines for member-created Web pages.

Use of the Internet is at your own risk, and AOL cannot be responsible for the content and conduct you may encounter. If the content or behavior originates outside the AOL community, we cannot remove it and are limited in the actions we can take. In addition, not every Web site you encounter will have a privacy policy and those that do may differ from AOL's. Be very careful about giving out personal information.

Since the Internet contains goods and services that may not be appropriate for minors (or some adults!), you may want to use our Parental Controls (Keyword: Parental Controls) to block access to certain parts of the Internet for your account or sub-accounts, especially if kids are online in your home.

International online areas.

AOL also allows you to visit AOL International areas online. These areas may have slightly different rules for conducting yourself and different standards for acceptable content. You should refer to the local rules in those areas; in general, "when in Rome" do as the folks do there. For example, harmless words in the United States might take on a completely different meaning in the United Kingdom. Guides or hosts in those areas may issue you a warning, and termination is possible if you violate the rules of the international area. Bear in mind that cyberspace law is evolving, so it's a good idea to review the rules of your favorite areas

frequently.

Getting help: Online resources.

Like the rest of the world, AOL may contain some material that is inappropriate for kids, young teens, or to some adults. Content in chat rooms is expressed immediately, so it can't be monitored in advance. Whether or not content is appropriate for children or for your tastes is up to you. We want to make sure that you have the ability to control what you or your children see.

AOL provides many online means of modifying the online environment, all of which can be controlled by the master account.

Parental Controls (Keyword: Parental Controls). Our Parental Controls allow the master account holder to adjust the online access of children on that account as they mature. You can designate each screen name as a child, young teen, mature teen, or 18+ account. Designating an account as a child or young teen account restricts your child's access to certain areas on AOL and the Internet (when accessed through AOL) and to Internet services available through America Online, such as online transactions. Each of these restrictions can be customized. But remember: No system of controls makes up for good old-fashioned parental supervision. We recommend that you monitor your child's use of AOL and that you make sure that your children understand AOL's Safety Tips.

Web Controls (Keyword: Parental Controls). Web Controls let you restrict your child's access to the World Wide Web. You can set controls to allow your child to go only to pre-approved sites, or prevent your teen from going to identified pornographic sites on the Web.

Mail Controls (Keyword: Mail Controls). Mail Controls allow you to:

* Block or allow all e-mail
* Block or allow e-mail from specific addresses or from the Internet
* Block domains (the sources of the mail)
* Block file attachments to e-mail

Marketing Preferences (Keyword: Marketing Preferences). AOL occasionally makes our membership mailing list available to companies whose products or services may be of interest to you. Marketing Preferences allows you to tell us if you do not want your name to be released to other organizations. You can also tell us if you do not want to receive member offers from AOL.

For more information about online safety and security, check out the following:

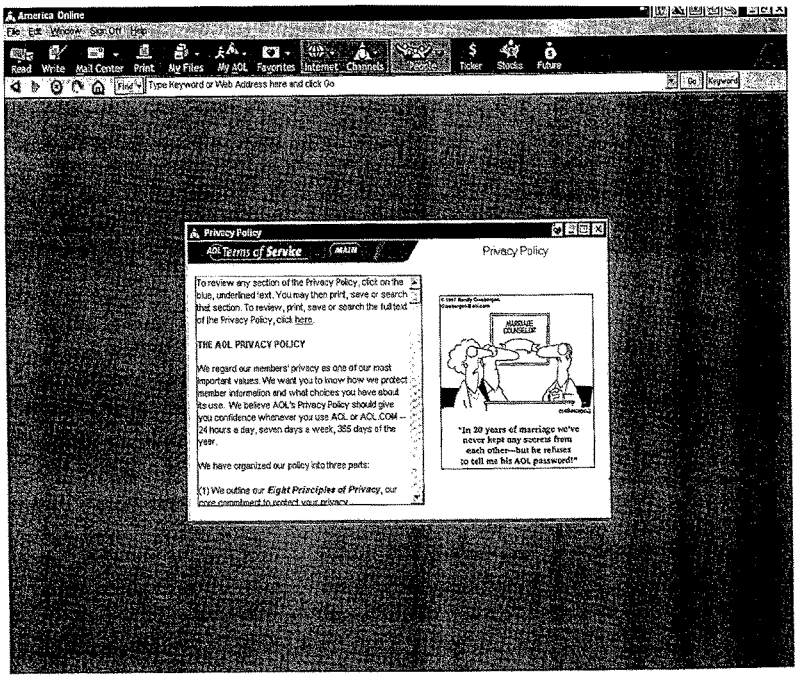
Neighborhood Watch (Keyword: Neighborhood Watch). Neighborhood Watch is your online area for information about online safety and security, dealing with issues such as viruses, keeping your account secure, reporting violations, or online conduct.

Member Services (Keyword: Help). This area has answers to a wide range of questions about AOL's service.

How to Notify AOL of Problems Online
There are two ways to inform AOL's Community Action Team (CAT) of violations you have either seen or been subject to online. AOL's CAT is a highly trained group responsible for educating and empowering members and for enforcing AOL's content and conduct standards. CAT can issue written warnings and, should the violation(s) be serious enough, terminate an account.

You can notify AOL of a violation by going to Keyword: Notify AOL or Keyword: I Need Help. Using Keywords: TOS or Keyword: Terms of Service allows you to review these guidelines.

When in a chat room, you can also click the **Notify AOL** button. This allows you to report a problem without having to leave your chat room.


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Ticker Stocks Future
Find Type Keyword or Web Address here and click Go
Go Keyword
Privacy Policy
AOL Terms of Service MAIN
Privacy Policy
To review any section of the Privacy Policy, click on the blue, underlined text. You may then print, save or search that section. To review, print, save or search the full text of the Privacy Policy, click here.
THE AOL PRIVACY POLICY
We regard our members' privacy as one of our most important values. We want you to know how we protect member information and what choices you have about its use. We believe AOL's Privacy Policy should give you confidence whenever you use AOL or AOL.COM -- 24 hours a day, seven days a week, 365 days of the year.
We have organized our policy into three parts:
(1) We outline our Eight Principles of Privacy, our
MARRIAGE COUNSELOR
"In 20 years of marriage we've never kept any secrets from each other—but he refuses to tell me his AOL password!"

We regard our members' privacy as one of our most important values. We want you to know how we protect member information and what choices you have about its use. We believe AOL's Privacy Policy should give you confidence whenever you use AOL or AOL.COM -- 24 hours a day, seven days a week, 365 days of the year.

We have organized our policy into three parts:

(1) We outline our ***Eight Principles of Privacy***, our core commitment to protect your privacy.

(2) We explain how we implement each principle. You can click on any principle to read the policy.

(3) We provide Helpful Tips on how you can better protect your privacy in cyberspace.

AOL'S PRIVACY COMMITMENT:
THE EIGHT PRINCIPLES OF PRIVACY

We are committed to protecting your personal privacy. Our Eight Principles of Privacy summarize and clarify that commitment: how we safeguard your privacy, how we treat personal information, and what choices you have. We understand that for you to take full advantage of the benefits of this interactive medium, we must do everything we can to ensure that your privacy is secure.

1. We do not read your private online communications.

2. We do not use any information about where you personally go on AOL or the Web, and we do not give it out to others.

3. We do not give out your telephone number, credit card information or screen names, unless you authorize us to do so. And we give you the opportunity to correct your personal contact and billing information at any time.

4. We may use information about the kinds of products you buy from AOL to make other marketing offers to you, unless you tell us not to. We do not give out this purchase data to others.

5. We give you choices about how AOL uses your personal information.

6. We take extra steps to protect the safety and privacy of children.

7. We use secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information.

8. We will keep you informed, clearly and prominently, about what we do with your personal information, and we will advise you if we change our policy.

(1) We do not read your private online communications.

AOL honors the confidentiality of its members' private communications in private chat rooms, e-mail (including downloads), and Instant Message(TM) conversations, as well as any profile data you may create, such as a stock portfolio. AOL does not read or disclose private communications except to comply with valid legal process such as a search warrant, subpoena or court order, to protect the company's rights and property, or during emergencies when we believe physical safety is at risk. Of course, what you write or post in public or member chat rooms and message boards is available not only to AOL, but to all members.

(2) We do not use any information about where you personally go on AOL or the Web, and we do not give it out to others.

Our system automatically gathers information about the areas you visit on our service.

We do not use any of this navigational data about where you -- as an individual member -- go on the service. Nor do we share

any of this data with outside companies.

We do use navigational information in the aggregate to understand how our members as a group use the service so that we can make AOL better. We may also share this statistical information with our partners or other outside companies, but in doing so, we don't disclose individual names or personal navigational information.

We do not keep track of where you go on the World Wide Web.

The Web sites you visit may have their own privacy policies or no policy at all. We encourage you to review the privacy policies of Web sites before providing them with any of your personal information.

(3) We do not give out your telephone number, credit card information or screen names, unless you authorize us to do so. And we give you the opportunity to correct your personal contact and billing information at any time.

When you join AOL, we ask you for your name, address, telephone number, and billing information-including the credit card, checking account, or debit card used to pay for your account -- and the various screen names you want to use on your account. Here is how we protect that information:

* AOL will not give out your telephone number or screen names (e-mail addresses), except where needed to deliver a product or service you ordered.

* We will not give out your credit or debit card number or checking account information unless you authorize it, for example, during an online purchase.

* We will not give out information that would link your screen names with your actual name.

We make lists of members' names and addresses available to pre-screened companies who have specific direct mail product and service offers we think may be of interest to you. We also sometimes combine these lists with publicly available information or segment them based on other information, such as when a member joined AOL or a member's computer system type. These lists are never based on a member's online activities.

You may choose to remove your name and address from the mailing lists we provide to other companies. For more information about your choices, please see Principle 5.

We also collect and use other information for internal purposes. For example, we keep records in your account history of your complaints about other members' online behavior, your contact with AOL Member Services and any reported violations of our Terms of Service (TOS) that you or someone on your account may have committed. AOL automatically queries your computer for information about your computer system such as the speed of your modem, error messages you may have received, or whether you use Macintosh(TM) or Windows(TM) software -- to help us fit the service to your individual needs and to help us diagnose problems you may be having with your system. Finally, we sometimes use information about your geographical location to provide localized service. For example, we may use your zip code or the time zone you are in to make sure the weather information or TV listings you see are accurate for you.

We have two exceptions to these policies: We will release specific information about your account only to comply with valid legal process such as a search warrant, subpoena or court order, or in special cases such as a physical threat to you or others.

We provide you with the opportunity to update or correct your contact and billing information that we have on file. Just as you want to make sure that information AOL has about you is accurate, we want to keep only the most up-to-date information about your account. Therefore, whenever you believe that your contact or billing information needs updating, you can go to Keyword: Billing and make the necessary changes.

(4) We may use information about the kinds of products you buy from AOL to make other marketing offers to you, unless you tell us not to. We do not give out this purchase data to others.

Your Purchases From AOL

AOL offers our members the opportunity to buy AOL store merchandise, such as computer hardware and software, and products

that carry the AOL brand. Like other retailers and direct marketers, we record information about such purchases. When you buy from us online, our system automatically gathers purchase data, and we also record information about purchases made through our telemarketing, mail order and other marketing operations.

We use this information in two ways:

1) We review what kinds of products and services appeal most to our members as a group. This statistical information helps us improve our offerings in the same way that other companies change their catalog based on what sells best.

2) We use information such as the number of purchases members make and the categories of goods and services they buy to make offers to you that we believe will interest you. In addition, we use other information such as when members joined AOL, how often they use the service or their type of computer system to make such offers. We also use publicly available consumer data to help us decide which marketing offers to make and which advertising they see.

You may choose not to receive marketing offers from AOL. For more information about your choices, please see Principle 5.

We do not give out any information about what you, as an individual, purchase from AOL, except to complete your transactions, or to comply with valid legal process such as a search warrant, subpoena or court order. We share with outside companies only statistical information about what AOL products or services our members -- as a group -- buy.

Your Purchases From AOL Certified Merchants

AOL Certified Merchants are required to provide a secure and safe environment for credit card purchases and will abide by AOL's privacy policy when handling any personal information given to them online by our members. These Certified Merchants will carry our AOL Guarantee Seal that tells you that you can conduct online business through AOL safely with them. Every time you make an online purchase from any AOL Certified Merchant, you are protected against liability in the unlikely event of credit card fraud. Simply follow your credit card company's reporting procedures, and AOL will reimburse you up to $50 for any remaining liability for unauthorized charges. Learn more at Keyword: Guarantee.

Your Other Online Purchases Through Our Service

For all other online purchases, be sure to review the merchants' privacy policies and contact them directly if you have any questions. They may have privacy terms that differ from AOL's privacy policy, and they may use personal information which you may provide them differently than our policy permits.

AOL may be involved in facilitating your purchases from these other companies, but this individual data is not used for any other purpose.

(5) We give you choices about how AOL uses your personal information.

You have choices about how the information you have provided may be used by us to make special offers to you. And you can direct us to remove your name and address from mailing lists we provide to selected, pre-screened companies.

To activate any of these marketing preferences, go to Keyword: Marketing Preferences or Keyword: Choice or click on the **My AOL** button on the toolbar at the top of your screen.

* You may choose not to receive marketing offers from AOL by U.S. mail.

* You may choose not to receive marketing offers from AOL by telephone.

* You may choose not to receive marketing offers from AOL by e-mail.

* You may choose not to receive marketing offers from AOL through online "pop-up screens."

* You may choose to have your name and address removed from any mailing lists that we provide to other companies.

(6) We take extra steps to protect the safety and privacy of children.

Young people need special safeguards and privacy protection. We realize they may not understand all the provisions of our policy or be able to make thoughtful decisions about the choices available to adult members. So we have special privacy policies to protect kids and teens using areas on the service specifically designed for them, including our Kids Only Channel. And we urge all parents to teach their children about protecting their personal information while online.

* In areas on the service designed for children 12 and under, AOL and its partners require prior parental consent (for example, by sending in a permission form by regular mail or by fax) before collecting or using names, addresses, telephone numbers or other information that identifies a child offline. In addition, prior to children using screen names on the AOL service, we require parental (master account) consent at the time the subaccount screen name is created. We do this so that parents are aware of and consent to how their children may use their screen names; for example, using the screen name to request an online newsletter, to post a message on a message board or to participate in a chat room.

In areas designed for teens 13 through 15, AOL and its partners may not collect names, addresses, telephone numbers or other personally identifiable information without disclosing how that information will be used and notifying teens that they should obtain permission from their parents before providing any information.

* Another way parents can control their child's experience online is AOL's Parental Controls (Keyword: Parental Controls). These simple, flexible tools allow parents to customize content and functionality to their child's maturity level.

Since one master account may have up to five screen names, we encourage all parents to use their master account to create separate screen names for each child. This allows the parent to customize AOL to their child's maturity level and content needs: Kids Only (recommended for children 12 and under); Young Teen (recommended for ages 13-15); or Mature Teen (recommended for ages 16-17).

* Unsolicited e-mail is a problem for everyone, but it is particularly a problem for children. This includes mail that could contain content you may not want your children to see, or mail that may ask for information you would not want your children to give out.

If you want to minimize the unsolicited e-mail your children receive, you can use Mail Controls (Keyword: Mail Controls) to block all e-mail from the Internet or to select the e-mail addresses from which you wish to allow your children to receive e-mail. Remember that screen names and information voluntarily given by children and teens in public chat rooms, e-mail exchanges, message boards, the Member Directory, and other online communications are publicly available and may be used by other parties to generate unsolicited e-mail.

You can learn more about how to ensure a safe and enjoyable online experience for you and your family at Keyword: Neighborhood Watch.

(7) We use secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information.

We use state-of-the-art technology to keep your personal information-including your billing and account information -- as secure as possible. We also have put in place privacy protection control systems designed to ensure that your personal data remain safe and private.

Each and every AOL employee must abide by AOL's privacy policy. Only authorized AOL employees are permitted to have access to your personal information and such access is limited by need. For example, if you call our Member Services department with a concern or complaint, the representative is allowed to access only the personal information that he or she needs to address your concern. In addition, any company with which AOL contracts to be our agent in conducting our business is required to adhere to confidentiality agreements to ensure that your information remains safe and secure.

All AOL employees are required to acknowledge that they understand and will comply with this privacy policy. Employees who violate our privacy policies are subject to disciplinary action, up to and including termination.

We strongly encourage our content, commerce and advertising partners to post clearly their own privacy policies and to have privacy control systems in place to protect your personal information. Be sure to review their privacy policies and contact them directly if you have any questions.

(8) We will keep you informed, clearly and prominently, about what we do with your personal information, and we

will advise you if we change our policy.

A key part of AOL's commitment to protecting your privacy is explaining to you how we may use your personal information. This privacy policy serves that purpose, and it is accessible through several means within our service. When you register for our service, you are presented with our privacy policy and should familiarize yourself with this and all other AOL policies at that time. In addition, this policy is easily located in our Terms of Service area (Keyword: TOS), and by using Keyword: Privacy, you can view AOL's privacy policy.

Whenever we change our policy, we will give you 30 days' notice of those changes through prominent disclosures, including notification on our front screen. If policy changes are substantial, we will notify each of our members individually through pop-up screens or e-mails. Since pop-ups last only for a limited time, however, you should sign on to your account regularly for these and other important announcements.

If you'd like to comment on or have questions about our privacy policy, or if you have a concern or policy violation you wish to report, please go to Keyword: Privacy Questions.

TEN TIPS TO HELP YOU PROTECT
YOUR PRIVACY AND SECURITY ONLINE

You can take the responsibility to protect your personal privacy online. Here is a checklist that will help safeguard your privacy and protect the integrity of your computer and AOL account. We urge you to print these tips and post them near your computer for you and your children.

_____ (1) Never give your password to anyone online. Never give your billing information except to facilitate a purchase.

_____ (2) Make your password at least 6 characters in length. Create a password that includes a combination of numbers and letters (such as sun8ray or bel3jar2 or 12hat93). Be sure to use different passwords for each screen name on your account.

_____ (3) If you have fallen for an online scam and given out your password, change your password right away. Before you sign off, go to Keyword: Password and create a new password for your screen name. Also, change the passwords for any other screen names on your account.

_____ (4) Setting up a Member Profile about yourself can be a good way of connecting with communities of AOL members. But be aware that Member Profiles are public. It's a good idea to avoid including information that could allow people to find you offline, such as your phone number or exact street address.

_____ (5) Use AOL's Mail Controls(TM) feature to control the e-mail you and your children receive. You can block e-mail from the Internet, entire domain names and specific e-mail addresses. You can even block the exchange of attached files or pictures in e-mail.

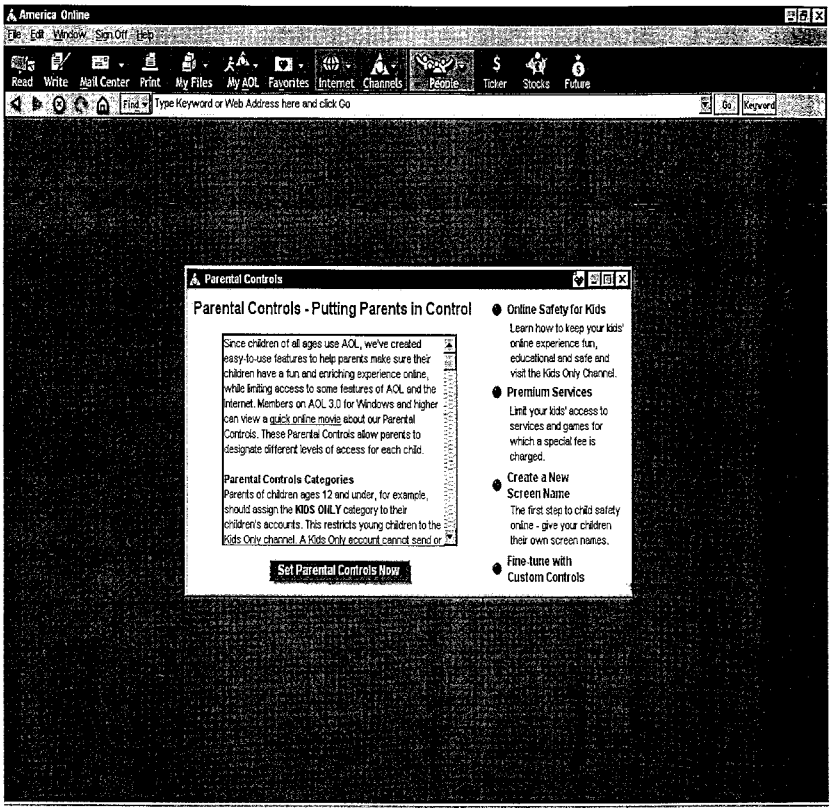
_____ (6) Your computer cannot catch a virus by opening a piece of e-mail. But if the e-mail asks for a password or billing information, or contains a file attachment from someone you don't know, go to Keyword: Notify AOL to learn how to report it.

_____ (7) Never download files unless you know what they are and who sent them to you. Computer viruses and destructive programs that could cause your computer to divulge personal information are often transferred in cleverly disguised files.

_____ (8) When you leave the AOL environment to go on the Web, you may want to check the sites you visit to see if they have a privacy policy. Take special care to protect your personal information and your screen name, since the operators of Web sites are not bound by AOL's privacy policy.

_____ (9) Explain to your children that some non-AOL contests could ask them for personal information, and make very clear what information they may or may not provide, under any circumstances.

_____ (10) You can get instructions to report any violation by going to Keyword: Notify AOL. You can get answers to common questions, and more tips for protecting yourself online, by going to Keyword: Neighborhood Watch.


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Ticker Stocks Future
Find Type Keyword or Web Address here and click Go
Go Keyword
Parental Controls
Parental Controls - Putting Parents in Control
Since children of all ages use AOL, we've created easy-to-use features to help parents make sure their children have a fun and enriching experience online, while limiting access to some features of AOL and the Internet. Members on AOL 3.0 for Windows and higher can view a quick online movie about our Parental Controls. These Parental Controls allow parents to designate different levels of access for each child.
Parental Controls Categories
Parents of children ages 12 and under, for example, should assign the KIDS ONLY category to their children's accounts. This restricts young children to the Kids Only channel. A Kids Only account cannot send or
Set Parental Controls Now
Online Safety for Kids
Learn how to keep your kids' online experience fun, educational and safe and visit the Kids Only Channel.
Premium Services
Limit your kids' access to services and games for which a special fee is charged.
Create a New Screen Name
The first step to child safety online - give your children their own screen names.
Fine-tune with Custom Controls

Since children of all ages use AOL, we've created easy-to-use features to help parents make sure their children have a fun and enriching experience online, while limiting access to some features of AOL and the Internet. Members on AOL 3.0 for Windows and higher can view a quick online movie about our Parental Controls. These Parental Controls allow parents to designate different levels of access for each child.

Parental Controls Categories
Parents of children ages 12 and under, for example, should assign the **KIDS ONLY** category to their children's accounts. This restricts young children to the Kids Only channel. A Kids Only account cannot send or receive Instant Message™ notes (private real-time communications), cannot enter member-created chat rooms, cannot use premium services, and can only send and receive text-only electronic mail (no file attachments OR embedded pictures allowed).

Parents of teenagers might want to select **YOUNG TEEN** (ages 13-15) or **MATURE TEEN** (16-17). These provide more freedom, while still preventing access to certain features. Young Teens may visit some chat rooms, but not member-created rooms or private rooms. Both groups are restricted to Web sites appropriate for their age categories. They are also blocked from Internet newsgroups that allow file attachments and they cannot use premium services.

Finally, the **18+** designation provides unrestricted access to all features on AOL and the Internet.

Note: These Parental Controls categories block e-mail attachments for some age groups but do not affect who your children can receive mail from. To control who can and cannot send e-mail to your children, click on **Fine-tune with Custom Controls**.

These age groups are guidelines. Since maturity levels of children vary, Parental Controls give you the flexibility to choose the right level of access for your child. For example, some parents may consider their 15 year old a "mature teen," while others may wish to maintain the "young teen" setting. It's up to you.

Custom Controls
After setting a control level, you can fine-tune the settings by using **CUSTOM CONTROLS**. This allows you to adjust specific activities, depending on the needs of your child, such as chat, the Web, e-mail, newsgroups and file downloads.

Remember that you may change the categories at any time, so you can adjust your children's access to best accommodate their maturity level or special needs.

Parental Controls Work by Screen Name
For Parental Controls to work, each child must have his or her own screen name. Your AOL account allows you to create up to five screen names. When you create a screen name, AOL automatically asks you to set a Parental Control level for that name. To create a screen name, sign on to AOL using a master screen name. (Master screen names are the first screen name you created when you joined AOL and any other screen names that have been designated as master screen names using Parental Controls.) Then click on the **Create a New Screen Name** button to the right.

If your children already have screen names, click on **Set Parental Controls Now** below.

Note: If your children use AOL immediately after you do, please sign off AOL, *then close and reopen the AOL software* before your children sign on with their own screen name. This ensures that all Parental Control settings will be in effect for that screen name.

Discussing Parental Controls
Parents can discuss their questions and share their online experiences regarding child safety on AOL and the Internet in our Message Boards.

The first step in setting Parental Controls for your children is to create a screen name for each child. When you create a new screen name, you will be asked to choose a Parental Control level for that name. To create a new screen name, click on the **Create a New Screen Name** button to the right.

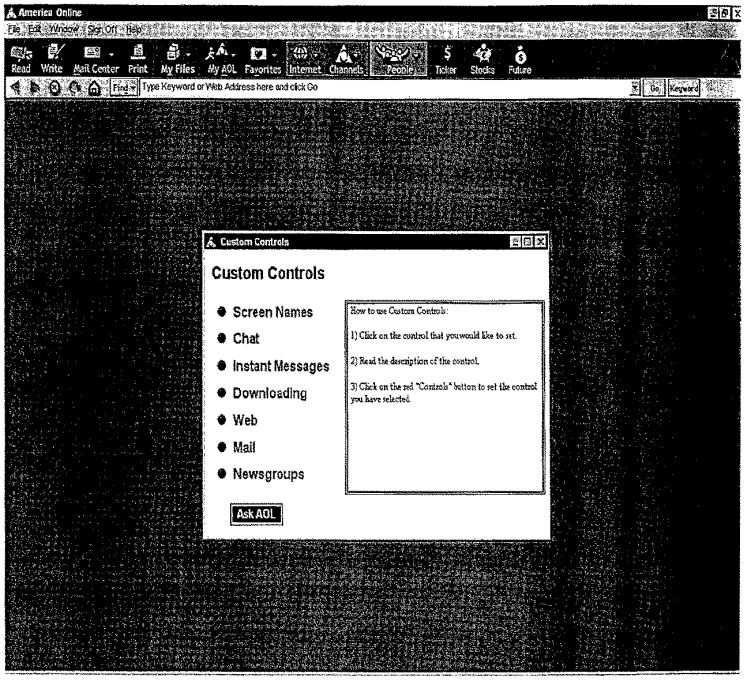
Once you've set the Parental Controls for each child's account, explore some of these additional ideas for creating a safe online experience for your children.

* **Store the password for your child's screen name, and don't tell them what it is.** The best way to prevent your child from revealing their password to others online, and possibly compromising your AOL account, is to store their password. When an AOL password is stored, it does not need to be typed each time you sign on to AOL. Your children will not need to know their password, and thereby won't give it out! To store an AOL password, click on the **My AOL** button to the right, select **Preferences** from the My AOL screen, then select **Your Password**. (Note: When you store your password, anyone with access to your computer can sign on to your AOL account. Don't store your password if others have access to your computer.)

* **Get to know your children's online world.** Spend some time with your children when they are online. Get to know their online friends and what online areas they visit, just as you know their neighborhood friends and what they watch on television. Recommend fun and educational online areas to your child. A great place to start is the award winning AOL Kids Only Channel. To visit the Kids Only Channel, click on the **Kids Only** button to the right.

Getting to know your children's online world can also help you tailor their Parental Control setting with Custom Controls. For example, you may decide to allow your teen to receive e-mail from AOL accounts only, and block Internet e-mail to their account. This is easy to do with Custom Controls.

Parental Controls are a great way to tailor your children's online experience to what's right for them, but there's no better safeguard than good old-fashioned parental supervision.


America Online
File Edit Window Sign Off Help
Read Write Mail Center Print My Files My AOL Favorites Internet Channels People Ticker Stocks Future
Find Type Keyword or Web Address here and click Go
Go Keyword
Custom Controls
Custom Controls
Screen Names
Chat
Instant Messages
Downloading
Web
Mail
Newsgroups
Ask AOL
How to use Custom Controls:
1) Click on the control that you would like to set.
2) Read the description of the control.
3) Click on the red "Controls" button to set the control you have selected.

○