PRIVACY ONLINE: A REPORT TO CONGRESS

FEDERAL TRADE COMMISSION

JUNE 1998

FEDERAL TRADE COMMISSION

Robert Pitofsky	Chairman
Mary L. Azcuenaga	Commissioner
Sheila F. Anthony	Commissioner
Mozelle W. Thompson	Commissioner
Orson Swindle	Commissioner

BUREAU OF CONSUMER PROTECTION

Authors

Martha K. Landesberg	Division of Credit Practices
Toby Milgrom Levin	Division of Advertising Practices
Caroline G. Curtin	Division of Advertising Practices
Ori Lev	Division of Credit Practices

Survey Advisors

Manoj Hastak	Division of Advertising Practices
Louis Silversin	Bureau of Economics
Don M. Blumenthal	Litigation and Customer Support Center Information and Technology Management Office
George A. Pascoe	Litigation and Customer Support Center Information and Technology Management Office

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- A medical clinic's online doctor-referral service invites consumers to submit their name, postal address, e-mail address, insurance company, any comments concerning their medical problems, and to indicate whether they wish to receive information on any of a number of topics, including urinary incontinence, hypertension, cholesterol, prostate cancer, and diabetes. The online application for the clinic's health education membership program asks consumers to submit their name, address, telephone number, date of birth, marital status, gender, insurance company, and the date and location of their last hospitalization. The clinic's Web site says nothing about how the information consumers provide will be used or whether it will be made available to third parties.

- A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The site also asks a child whether he or she has received gifts in the form of stocks, cash, savings bonds, mutual funds, or certificates of deposit; who has given these gifts; whether monetary gifts were invested in mutual funds, stocks, or bonds; and whether the child's parents own mutual funds. Elsewhere on the site, contest winners' full name, age, city, state and zip code are posted. The Web site does not tell children to ask their parents for permission before providing personal information and does not appear to take any steps to involve parents. Further, the site says nothing about whether the information is disclosed to third parties.

*** * ***

The World Wide Web is an exciting new marketplace for consumers. It offers easy access to a broad array of goods, services, and information, but also serves as a source of vast amounts of personal information about consumers, including children. While the online consumer market is growing exponentially, there are also indications that consumers are wary of participating in it because of concerns about how their personal information is used. As the above examples show, these concerns are real, for both adults and children.

The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace and has held a series of workshops and hearings on such issues. Throughout, the Commission's goal has been to encourage and facilitate effective self-

regulation as the preferred approach to protecting consumer privacy online. These efforts have been based on the belief that greater protection of personal privacy on the Web will not only protect consumers, but also increase consumer confidence and ultimately their participation in the online marketplace. In this report, the Commission summarizes widely-accepted principles regarding information collection, use, and dissemination; describes the current state of information collection and privacy protection online; and assesses the extent of industry's self-regulatory response.

Government studies in the United States and abroad have recognized certain core principles of fair information practice. These principles are widely accepted as essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests. These core principles require that consumers be given *notice* of an entity's information practices; that consumers be given *choice* with respect to the use and dissemination of information collected from or about them; that consumers be given *access* to information about them collected and stored by an entity; and that the data collector take appropriate steps to ensure the *security* and integrity of any information collected. Moreover, it is widely recognized that fair information practice codes or guidelines should contain enforcement mechanisms to ensure compliance with these core principles. With respect to the collection of information from children, a wide variety of public policies recognize the important supervisory role of parents in commercial transactions involving their children. Parental control is also the touchstone for application of fair information practice policies to the collection of information from children.

The Commission solicited industry association fair information practice guidelines to assess their conformity with these core principles. This assessment shows that industry association guidelines generally encourage members to provide notice of their information practices and some choice with respect thereto, but fail to provide for access and security or for enforcement mechanisms.

The Commission also examined the practices of commercial sites on the World Wide Web. The Commission's survey of over 1,400 Web sites reveals that industry's efforts to encourage

voluntary adoption of the most basic fair information practice principle — notice — have fallen far short of what is needed to protect consumers. The Commission's survey shows that the vast majority of Web sites — upward of 85% — collect personal information from consumers. Few of the sites — only 14% in the Commission's random sample of commercial Web sites — provide any notice with respect to their information practices, and fewer still — approximately 2% — provide notice by means of a comprehensive privacy policy. The results with respect to the collection of information from children are also troubling. Eighty-nine percent of children's sites surveyed collect personal information *from children*. While 54% of children's sites provide some form of disclosure of their information practices, few sites take any steps to provide for meaningful parental involvement in the process. Only 23% of sites even tell children to seek parental permission before providing personal information, fewer still (7%) say they will notify parents of their information practices, and less than 10% provide for parental control over the collection and/or use of information from children. The Commission's examination of industry guidelines and actual online practices reveals that effective industry self-regulation with respect to the online collection, use, and dissemination of personal information has not yet taken hold.

In light of the Commission's findings and significant consumer concerns regarding privacy online, it is evident that substantially greater incentives are needed to spur self-regulation and ensure widespread implementation of basic privacy principles. The Commission is currently considering such incentives and possible courses of action to adequately protect the privacy of online consumers generally. The Commission will make its recommendations on this subject this summer.

In the specific area of children's online privacy, however, the Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children. Such legislation would require Web sites that collect personal identifying information from children to provide actual notice to parents and obtain parental consent. The timing of such notice and consent would vary depending on the age of the child, and the nature and uses of the information collected. Such legislation would protect children and ensure that parents have knowledge of, and control over, the collection of

information from their children.

The development of the online marketplace is at a critical juncture. If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential. To date, industry has had only limited success in implementing fair information practices and adopting self-regulatory regimes with respect to the online collection, use, and dissemination of personal information. Accordingly, the Commission now recommends legislation to protect children online and this summer will recommend an appropriate response to protect the privacy of all online consumers.

I. INTRODUCTION

This report to Congress provides an assessment of the effectiveness of self-regulation as a means of protecting consumer privacy on the World Wide Web ("the Web").[1] It is based on a comprehensive online survey of the information practices of commercial Web sites, including sites directed to children, conducted in March 1998; an examination of current industry guidelines governing information practices online; and the record developed in Commission hearings and workshops held since 1995.

Part II of the report provides a brief history of the Commission's work in the area of online privacy, and a summary of the privacy concerns raised by the new online marketplace. Part III describes what have come to be recognized as the core principles of privacy-protective information practices. Part IV then compares current industry guidelines with these generally accepted principles, and Part V presents the findings of the Commission's survey of Web sites. Part VI sets forth the Commission's conclusions.

II. HISTORY AND OVERVIEW

A. THE FEDERAL TRADE COMMISSION'S APPROACH TO ONLINE PRIVACY

The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace. In April 1995, staff held its first public workshop on privacy on the Internet, and in November of that year the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues.

In June 1996, the Commission conducted a two-day workshop to explore privacy concerns raised by the online collection of personal information, and the special concerns raised by the collection of personal information from children. The workshop considered an array of alternatives to address those concerns, including industry self-regulation, technology-based solutions, consumer and business education, and government regulation. A summary of the workshop testimony was published by the Commission in a December 1996 staff report entitled *Consumer Privacy on the Global Information Infrastructure*. A second workshop in June 1997 delved more deeply into these issues.[2] In all of these endeavors the Commission's goals have been (1) to identify potential consumer protection issues related to online marketing and commercial transactions; (2) to provide a public forum for the exchange of ideas and presentation of research and technology; and (3) to encourage effective self-regulation.[3]

B. CONSUMER PRIVACY ONLINE

1. GROWTH OF THE ONLINE MARKET

The World Wide Web is an exciting new marketplace for consumers. It offers easy access not only to a vast array of goods and services, but also to rich sources of information that enable

consumers to make better-informed purchasing decisions. It also offers the convenience of shopping from the office or home. This information-rich medium also serves as a source of vast amounts of personal information about consumers. Commercial Web sites collect personal information explicitly through a variety of means, including registration pages, user surveys, and online contests, application forms, and order forms. Web sites also collect personal information through means that are not obvious to consumers, such as "cookies."[4]

The online consumer market is growing exponentially. In early 1997, 51 million adults were already online in the U.S. and Canada,[5] and 73% reported that they had shopped for product information on the World Wide Web.[6] By December 1997, the number of adults online in the U.S. and Canada had climbed to 58 million, and 10 million had actually purchased a product or service online.[7] Analysts estimate that Internet advertising — which totaled approximately $301 million in 1996 — will swell to $4.35 billion by the year 2000.[8]

2. PRIVACY CONCERNS

While these figures suggest that the online marketplace is growing rapidly, there are also indications that consumers are wary of participating in it. Surveys have shown that increasing numbers of consumers are concerned about how their personal information is used in the electronic marketplace. This research indicates that consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information.[9] In fact, a substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are.[10] According to the results of a March 1998 *Business Week* survey, consumers not currently using the Internet ranked concerns about the privacy of their personal information and communications as the top reason they have stayed off the Internet.[11] Clearly, consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections.[12] These findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until

meaningful and effective consumer privacy protections are implemented in the online marketplace. If such protections are not implemented, the online marketplace will fail to reach its full potential.

C. CHILDREN'S PRIVACY ONLINE

1. GROWTH IN THE NUMBER OF CHILDREN ONLINE

Children represent a large and rapidly growing segment of online consumers and are being actively targeted by commercial Web sites.[13] Children use the Web for a wide variety of activities, including homework, informal learning, browsing, playing games, corresponding with electronic pen pals by e-mail, placing messages on electronic bulletin boards and participating in chat rooms.[14] Among the activities most attractive to children are those that allow them to communicate directly with their peers, for example, chat rooms, bulletin boards and e-mail.[15] Almost 10 million (14%) of America's 69 million children are now online, with over 4 million accessing the Internet from school and 5.7 million from home.[16] Children are also avid consumers and represent a large and powerful segment of the marketplace. They are estimated to spend billions of dollars a year, and to influence the expenditure of billions more.[17] Their growing presence online, therefore, creates enormous opportunities for marketers to promote their products and services to an eager audience.[18] At the same time, the Web offers an easy way to collect large amounts of detailed marketing data from and about children.

2. SAFETY AND PRIVACY CONCERNS

A wide variety of detailed personal information is being collected online from and about children, often without actual notice to or an opportunity for control by parents.[19] This information may be collected from children at various places on a site: when the child is registering for a contest, enrolling in an electronic pen pal program, completing a survey, or playing a game. A child may also reveal such personal information in the course of participating in chat rooms or posting messages on electronic bulletin boards — areas that are publicly accessible to anyone surfing the Web.[20] These practices present unique privacy and safety

concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent.

The most potentially serious safety concern is presented by the posting of personal identifying information by and about children — *i.e.*, information that can be used to identify children, such as name, postal or e-mail address — in interactive public areas, like chat rooms and bulletin boards, that are accessible to all online users. These activities enable children to communicate freely with strangers, including adults. The FBI and Justice Department's "Innocent Images" investigation has revealed that online services and bulletin boards are quickly becoming the most powerful resources used by predators to identify and contact children.[21] Further, anecdotal evidence indicates that many children surfing the Web claim to have experienced problems such as attempted password theft and inappropriate advances by adults in children's chat rooms.[22]

Traditionally, parents have instructed children to avoid speaking with strangers. The collecting or posting of personal information in chat rooms and on bulletin boards online runs contrary to that traditional safety message. Children are told by parents not to talk to strangers whom they meet on the street, but they are given a contrary message by Web sites that encourage them to interact with strangers in their homes via the Web. The dangers in the Web environment are heightened by the fact that children cannot determine whether they are dealing with another child or an adult posing as a child.

In addition to these safety issues are privacy concerns raised by commercial Web sites' collection of personal information from children for marketing purposes. As described below, the practice is widespread and includes the collection of personal information from even very young children without any parental involvement or awareness.

There is considerable concern about online collection practices that bypass parents, who have traditionally protected children from marketing abuses.[23] Children generally lack the developmental capacity and judgment to give meaningful consent to the release of personal information to a third party.[24] This is an even greater problem when children are offered an

incentive for releasing personal information, or when release of personal information is a prerequisite to registering for a contest, joining a kid's club, or playing a game.[25]

Survey data confirm that parents strongly favor limiting the collection and use of personal information from and about their children. For example, 97% of parents whose children use the Internet believe Web sites should not sell or rent personal information relating to children, and 72% object to a Web site's requesting a child's name and address when the child registers at the site, even if such information is used only internally.[26]

In sum, the immediacy and ease with which personal information can be collected from children online, combined with the limited capacity of children to understand fully the potentially serious safety and privacy implications of providing that information, have created deep concerns about current information practices involving children online.

III. FAIR INFORMATION PRACTICE PRINCIPLES

A. FAIR INFORMATION PRACTICE PRINCIPLES GENERALLY

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information — their "information practices" — and the safeguards required to assure those practices are fair and provide adequate privacy protection.[27] The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.[28] Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. NOTICE/AWARENESS

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.[29] Moreover, three of the other principles discussed below — choice/consent, access/participation, and enforcement/redress — are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.[30]

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;[31]
- identification of the uses to which the data will be put;[32]
- identification of any potential recipients of the data;[33]

- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);[34]
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information;[35] and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[36]

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data;[37] whether the consumer has been given a right of access to the data;[38] the ability of the consumer to contest inaccuracies;[39] the availability of redress for violations of the practice code;[40] and how such rights can be exercised.[41]

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. CHOICE/CONSENT

The second widely-accepted core principle of fair information practice is consumer choice or consent.[42] At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — *i.e.*, uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer.[43] Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.[44] Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.[45]

3. ACCESS/PARTICIPATION

Access is the third core principle. It refers to an individual's ability both to access data about him or herself — *i.e.*, to view the data in an entity's files — and to contest that data's accuracy and completeness.[46] Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.[47]

4. INTEGRITY/SECURITY

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.[48]

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.[49] Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.[50]

5. ENFORCEMENT/REDRESS

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.[51] Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.[52]

a. Self-Regulation[53]

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).[54] Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;[55] external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.[56] A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.[57]

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.[58] Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.[59]

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (*e.g.*, correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer.[60] Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation.[61] The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, *e.g.*, the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages;[62] and the elements of any such cause of action.

c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers.[63] Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.[64]

B. APPLICATION OF FAIR INFORMATION PRACTICE PRINCIPLES TO INFORMATION COLLECTED FROM CHILDREN

The fair information practice codes discussed above do not address personal information collected from children. They are, however, applicable to parents, in light of the special status that children generally have been accorded under the law. This status as a special, vulnerable group is premised on the belief that children lack the analytical abilities and judgment of adults.[65] It is evidenced by an array of federal and state laws that protect children, including those that ban sales of tobacco and alcohol to minors, prohibit child pornography, require parental consent for medical procedures, and make contracts with children voidable. In the specific arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize both the need for heightened protections for children and the special role that parents play in implementing these protections.[66]

1. PARENTAL NOTICE/AWARENESS AND PARENTAL CHOICE/CONSENT

It is *parents* who should receive the notice and have the means to control the collection and use of personal information from their children. The Commission staff set forth this principle in a July 15, 1997 letter to the Center for Media Education.[67] In addition, the letter identifies certain practices that appear to violate the Federal Trade Commission Act:

(a) It is a deceptive practice to represent that a site is collecting personal identifying information from a child for a particular purpose (*e.g.* to earn points to redeem a premium), when the information will also be used for another purpose that parents would find material, in the absence of a clear and prominent disclosure to that effect; and

(b) It is likely to be an unfair practice to collect personal identifying information, such as a name, e-mail address, home address, or phone number, from children and to sell or otherwise disclose such identifying information to third parties, or to post it publicly

> online, without providing parents with adequate notice and an opportunity to control the collection and use of the information through prior parental consent.

This letter applies the Commission's Section 5 authority for the first time to the principles of notice and choice in the online collection of information from children. The principles set out in the staff opinion letter form an appropriate basis for public policy in this area.

To assure that notice and choice are effective, a Web site should provide *adequate notice* to a parent that the site wishes to collect personal identifying information from the child,[68] and give the parent an opportunity to control the collection and use of that information. Further, according to the staff opinion letter, in cases where the information may be released to third parties or the general public, the site should obtain the parent's *actual or verifiable consent*[69] to its collection.[70]

The content of the notice should include at a minimum, the elements described above,[71] but, in addition, should take into account the fact that online activities may be unique and unfamiliar to parents. Thus, a notice should be sufficiently detailed to tell parents clearly the type(s) of information the Web site collects from children and the steps parents can take to control the collection and use of their child's personal information. Where a Web site offers children interactive activities such as chat, message boards, free e-mail services, posting of home pages and key pal programs, it should explain to parents the nature of these activities and that children's participation enables others to communicate directly with them. Such notice empowers parents to monitor their children's interactions and to help protect their children from the risks of inappropriate online interactions.

2. ACCESS/PARTICIPATION AND INTEGRITY/SECURITY

Since parents may not be fully aware of what personal information a site has collected from their child, the access/participation principle is a particularly important one with respect to information collected from children. To provide informed consent to the retention and/or use of information collected from their children, parents need to be given access to the information collected from their children, particularly if any of the information is collected prior to providing notice to the parent. The principle of integrity, which addresses the accuracy of the data, is also

important for children's information. Parents have an interest in assuring that whatever information Web sites collect from children or have otherwise obtained about their children is accurate. This is particularly important in contexts that involve decisions that impact on the child or family, such as educational or health decisions. In addition, since children's information is considered to be a more sensitive type of information, sites should take the same steps identified above to assure that children's data is secure from unauthorized uses or disclosures.

IV. INDUSTRY ASSOCIATION GUIDELINES

Throughout the series of Commission workshops on online privacy issues, the online industry has asserted that self-regulation is a more efficient and effective means of creating online privacy protections than government regulation. To gauge the status and effectiveness of current self-regulatory efforts, on March 5, 1998 the Commission published a *Federal Register* Notice (the "Notice") requesting that trade associations and industry groups voluntarily submit copies of their online information practice guidelines and principles.[72] Nine industry-specific guidelines were submitted.[73] Copies of these guidelines are included in Appendix E. The guidelines do not address all of the core fair information practice principles discussed above, but all encourage companies to provide notice of at least some of their information practices, and most encourage choice with respect to the disclosure of personal information to third parties. For the most part, the submitted guidelines do not address access or security. Most importantly, very few provide any kind of enforcement mechanism, an essential element of effective self-regulation.

A. INDUSTRY ASSOCIATION GUIDELINES

1. NOTICE/AWARENESS

All of the guidelines submitted encourage member companies to provide at least some notice of their information practices. The extent of the suggested notice ranges from a general recommendation to post a privacy policy on Web sites,[74] to more specific exhortations to provide notice with respect to the nature of information collected, how it is collected, its intended uses, the nature and purposes of any intended disclosures to third parties, and the mechanism to opt-out of any third-party disclosure.[75] None of the guidelines discusses the need to provide notice about access or security.

2. CHOICE/CONSENT

Most of the guidelines suggest that member companies provide some degree of choice with respect to the use of personal information.[76] Here too there is a range in what is suggested by the guidelines. Some guidelines suggest giving consumers choice with respect to most secondary uses of their information, both external (*i.e.*, disclosure to third parties) and internal (*i.e.*, marketing back to the consumer);[77] others suggest giving consumers a choice solely with respect to external uses.[78] All of the guidelines speak of choice in terms of opt-out options for the consumer; none adopts an opt-in regime for adult consumers.

3. ACCESS/PARTICIPATION

Several of the industry guidelines address consumer access to information by providing generally that procedures should be established to ensure accuracy of the information, including allowing consumers access to, and the opportunity to correct, information collected about them.[79] Other guidelines fail to make any reference to the access principle.

4. INTEGRITY/SECURITY

Only the banking and financial industry association guidelines, and the individual reference services guidelines, make any reference to security issues. These guidelines call generally for appropriate security procedures, including the limitation of employee access to data.[80]

5. ENFORCEMENT/REDRESS

With limited exception,[81] the submitted guidelines contain no enforcement mechanisms. Only one of the guidelines conditions further membership and information sharing on adherence to the guidelines.[82] One other set of guidelines provides for peer review of alleged violations, but it is not binding.[83] All of the other guidelines and policies submitted are merely exhortatory.[84] As discussed above, the absence of enforcement mechanisms significantly weakens the effectiveness of industry-promulgated guidelines as a self-regulatory tool. This is especially true if member companies fail to voluntarily adhere to suggested policies.

B. GUIDELINES REGARDING CHILDREN'S INFORMATION

The Commission received two sets of guidelines regarding collection and use of information from children in response to its March 1998 Notice: the Children's Advertising Review Unit of the Council of Better Business Bureaus, Inc.'s ("CARU") *Guidelines for Interactive Electronic Media* ("*CARU Guidelines*") and the Direct Marketing Association's ("DMA") *Online Data Collection from or about Children* ("*DMA Children's Guidelines*").[85] Both guidelines address younger children.[86]

The *CARU Guidelines*, issued in April 1997, are consistent with the principles outlined in the staff opinion letter described above. They require that advertisers make "reasonable efforts" to provide notice and choice to parents when information is collected from children online, including the collection of information through "passive tracking."[87] In all cases, the notice must specify the means by which parents can correct or remove the information collected from a company's database.[88] The guidelines require prior parental consent (opt-in) to the collection of personal identifying information from children under the following circumstances: (1) when the information would enable the recipient to contact the child offline, regardless of the intended use; (2) when the information would be publicly posted so as to enable others to communicate directly with the child online; and (3) when the information would be shared with third parties.[89] Under other circumstances, such as the collection for internal use of an e-mail address, first name, or hometown, the site must provide notice to the parent and an opportunity to opt-out.[90] If a site collects only anonymous or aggregate information, the guidelines require notice of the intended uses of the information, but not parental consent.[91]

In addition, CARU has an enforcement mechanism in place to promote compliance with its online privacy guidelines,[92] and has achieved a remarkably high level of compliance under this mechanism in the offline media over a long period of time.[93] While CARU has worked to encourage Web sites to adhere to its privacy guidelines with respect to the collection of personal information from children online, to date it has not achieved the same widespread adherence it has achieved in other media.[94]

The *DMA Children's Guidelines*, which were adopted in January 1997, do not conform to the principles set forth in the staff opinion letter. The DMA is working now, however, to strengthen and refine its children's guidelines. The current *DMA Children's Guidelines* urge marketers to: (1) take into account a child's age, knowledge, sophistication, and maturity when collecting information; (2) encourage young children to obtain their parents' permission;[95] and (3) support parental control over the collection of data from children through notice and opt-out.[96] These guidelines do not call for *actual* notice to parents or for prior parental consent, even where the information is disclosed to third parties or otherwise made publicly available.

V. SURVEY OF COMMERCIAL WEB SITES

A. OVERVIEW

With these fair information practice principles and industry guidelines as background, the Commission conducted a survey of commercial sites on the World Wide Web. In July 1997, the Commission set out the objective of this survey: to determine whether self-regulation is an effective means of protecting consumer privacy on the Web. The Commission stated that it would measure the effectiveness of self-regulation by determining how many commercial Web sites are providing notice of their information practices and offering consumers choice regarding the collection and use of their personal information online.[97] To that end, in March 1998 Commission staff conducted an online survey of 1,402 commercial Web sites, including 212 sites directed to children.

The survey consists of six samples — group A, drawn from all commercial U.S. sites "likely to be of interest to consumers;" groups B, C, and D, drawn from all such sites in the health, retail, and financial sectors, respectively;[98] group E, drawn from all commercial U.S. sites "primarily directed to children aged fifteen or younger;" and group F, which includes the most popular U.S. commercial sites.[99] There are 674 sites in the Comprehensive Sample (group A), 137 sites in the Health Sample (group B), 142 sites in the Retail Sample (group C), 125 sites in the Financial Sample (group D), 212 sites in the Children's Sample (group E), and 111 sites in the Most Popular Sample (group F). A detailed methodology describing the survey sample selection, data collection, and validation procedures is included in Appendix A. A list of the sites included in each sample is included in Appendix C.

Forty Commission staff members [hereinafter "surfers"] surveyed the sites in each of the samples in the two-week period from March 9-20, 1998. Once a surfer concluded that a site qualified for inclusion in one of the samples (*i.e.*, it was "likely to be of interest to consumers" or was "primarily directed to children aged fifteen or younger"), the surfer searched the site to determine whether it collects personal information from online consumers and, if so, to ascertain

the kinds of information it collects and whether it discloses its information practices.[100] In the case of sites directed to children, personal information collected on a payment form was deemed to be collected from adults; all other personal information sought by children's sites was considered to be collected from children.

For purposes of this survey, "personal information" was defined to include two broad information categories: information that can be used to identify consumers, such as name, postal or e-mail address ("personal identifying information"); and demographic and preference information (such as age, gender, income level, hobbies, or interests) that can be used either in aggregate, non-identifying form for purposes such as market analysis, or in conjunction with personal identifying information to create detailed personal profiles of consumers.

To determine whether Web sites are giving consumers notice of their information practices and offering consumers choice, Commission staff searched Web sites for information practice disclosures. Such disclosures might be found in a "Privacy Policy Notice," defined as a comprehensive description of a site's information practices that is located in one place on the site and may be reached by clicking on an icon or hyperlink. Disclosures might also take the form of a discrete "Information Practice Statement," defined as a statement that describes a particular use or practice regarding consumers' personal information, or regarding a choice offered to consumers about their personal information, that might appear in diverse locations on the site. Examples of such disclosures include statements such as the following:

- We keep all the information you provide us confidential.
- We will only use the information you provide us to process your order.
- We [will, sometimes, never] share your information with third parties.

Staff also counted as an Information Practice Statement any disclosure that did not explicitly state how the personal information collected might be used, but nevertheless arguably raised an inference of at least one potential use. Statements such as "Click here to be on our mailing list" were, therefore, included as Information Practice Statements. Sites in the Children's Sample were analyzed to determine the nature of information collected from children and the extent of notice and/or choice offered to parents. Copies of the survey instructions and survey forms are included

in Appendices B and C, respectively. The survey results are set forth in the survey forms included in Appendix C and in the tables included in Appendix D.

B. GENERAL SURVEY FINDINGS

This section of the report describes the survey results for all sites other than those directed to children. It describes the types of companies whose sites are in each of the four random samples and in the sample of the most popular sites on the Web; the types of personal information collected by these sites; and the frequency and nature of information practice disclosures within each of these samples.

1. WEB SITES

The Comprehensive Sample (Sample A) includes 674 Web sites, and the types of companies included range broadly across the entire spectrum of the American economy. Bookstores, travel agencies and hardware stores, radio and television stations, manufacturers of foods and home health care products, clothing and sports equipment retailers, computer and software developers, online newspapers and magazines, auto dealerships and law firms, and sellers of all manner of other consumer goods and services are included in the Comprehensive Sample. Approximately 37% of the sites in the Comprehensive Sample are operated by small companies (annual sales less than $500,000.00), 40% by medium-sized companies (annual sales exceeding $500,000.00 but less than $10 million), and 20% by large companies (annual sales exceeding $10 million).[101]

The Health, Retail, and Financial Samples (Samples B, C, and D, respectively) are random samples of over 100 sites drawn from industry sectors in which consumers may have heightened concerns for privacy due to the types of personal information such Web sites are likely to collect: health-related sites may collect sensitive medical information; retail sites often collect credit card numbers; and sites offering financial services often collect account and asset-related information.

The Health Sample (Sample B) includes 137 sites operated by drug manufacturers, doctor's offices, hospitals, outpatient clinics, health maintenance organizations, manufacturers and retailers of health care products and non-prescription drugs, sellers of nutritional supplements, weight loss

centers, substance abuse treatment centers, and health information and referral services. Small, medium, and large businesses are nearly equally represented in the Health Sample (32% small; 35% medium-sized; and 31% large).[102]

The Retail and Financial Samples (Samples C and D) are similarly diverse. The range of consumer goods and services sold by the companies represented in the Retail Sample (Sample C) mirrors the variety found in the Comprehensive Sample. Sellers of photographic equipment, automobiles, cigars, jewelry, clothing, computers and software, fine art, collectibles, books, housewares and sheet music are represented, as are magazines, restaurants, sporting goods stores, and pharmacies. Forty percent of the 142 companies in the Retail Sample are small, 37% medium-sized, and 21% large.[103] The Financial Sample (Sample D) includes 125 sites operated by banks, credit unions, mortgage companies, real estate agencies, security and stock brokerages, investment and asset management firms, venture capital firms, investment counselors, stock exchanges, student loan services, and investment newsletters. Eighteen percent of the sites in the Financial Sample are associated with small companies, 41% with medium-sized companies, and 39% with large companies.[104]

The Most Popular Sample (Sample F) includes 111 of the most popular sites on the Web. Companies represented in this sample include search engines, Internet service providers, electronic mail services, software and computer companies, news and information companies, online directories, entertainment companies, and retailers of consumer goods.[105]

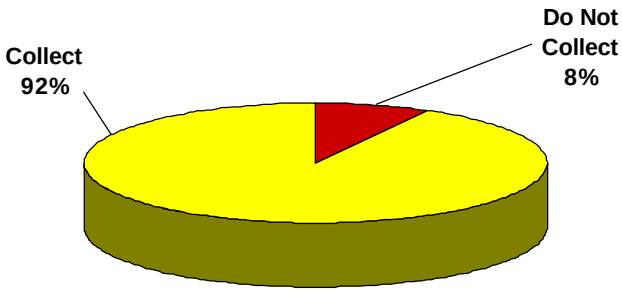
2. PERSONAL INFORMATION COLLECTION

As noted above, in the three years since the Commission's first workshop on online privacy issues, there has been substantial survey research indicating that consumers are concerned that commercial Web sites are collecting a great quantity of personal information online and that this practice might infringe on consumers' privacy.[106] The Commission's own survey findings demonstrate that, indeed, a significant amount of personal information is being collected from online consumers.

As the findings on information collection are consistent across all four random samples and the Most Popular Sample, they are discussed together here. Almost all of the sites in these samples — between 87% and 97% — collect at least one type of personal information from online consumers.[107] The vast majority of sites in all samples collect several types of personal information. Figure 1 shows the percent of sites in the Comprehensive Sample that collect personal information; Figure 1A provides this information for all of the random samples and the Most Popular Sample.

Figure 1

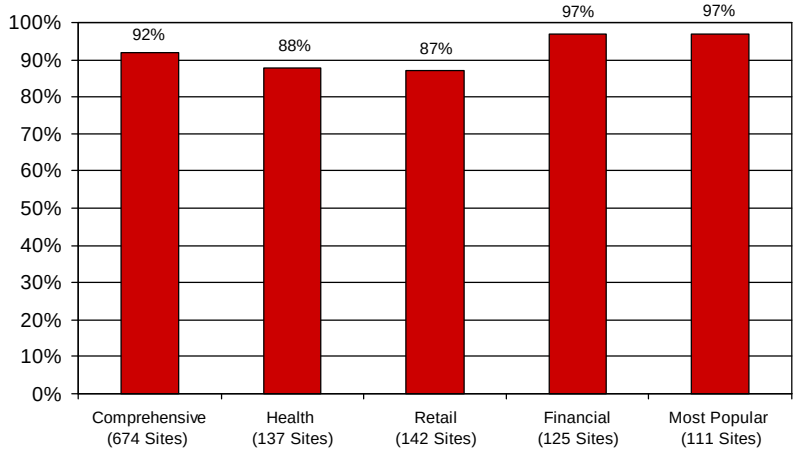
Percent of Web Sites Collecting Personal Information
Comprehensive Sample



Base: All Web Sites in Comprehensive Sample (674) **March 1998**

Figure 1A

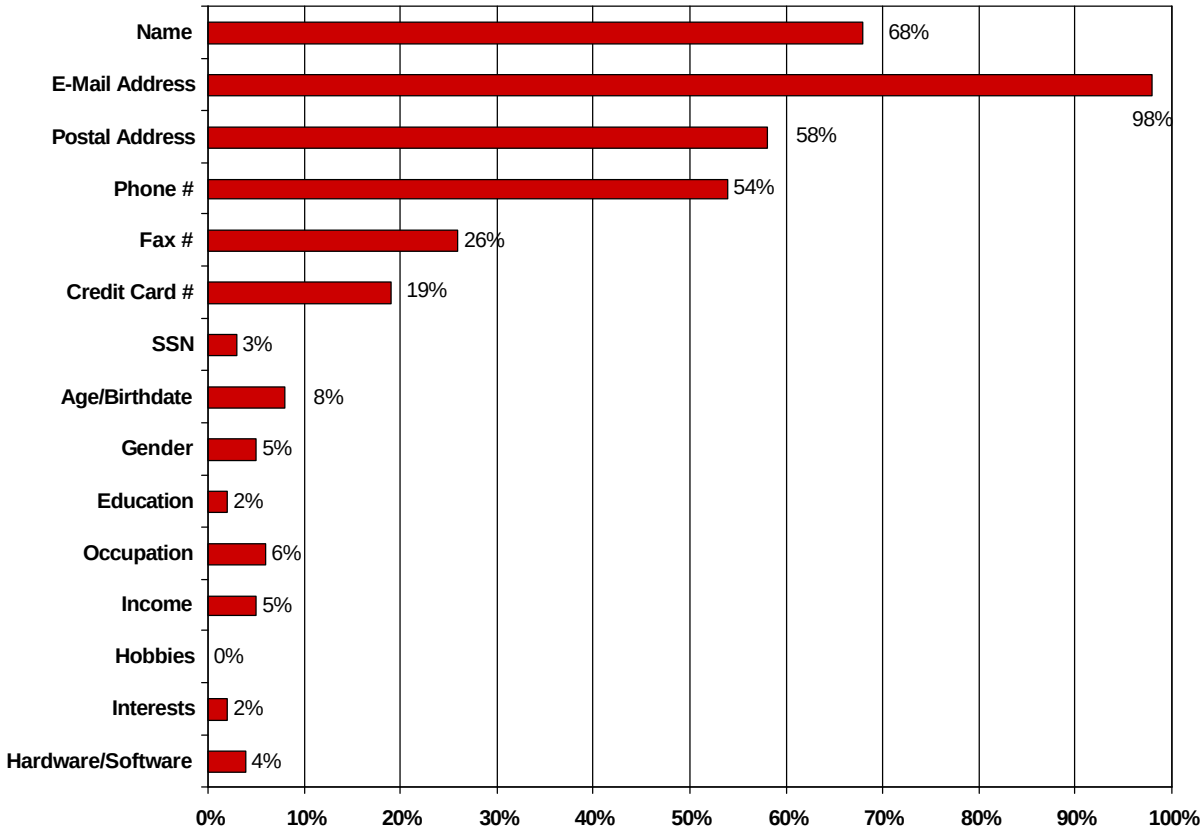
Percent of Web Sites Collecting Personal Information, By Sample



These Web sites collect a remarkable variety of personal information, including name, e-mail address,[108] postal address, telephone number, fax number, credit card number, Social Security number, age or date of birth, gender, education, occupation, income, hobbies, interests, and the type of hardware or software used by the online consumer. Figure 2 shows the percent of sites in the Comprehensive Sample that collect each type of personal information.[109]

Figure 2

Types of Personal Information Collected
Comprehensive Sample

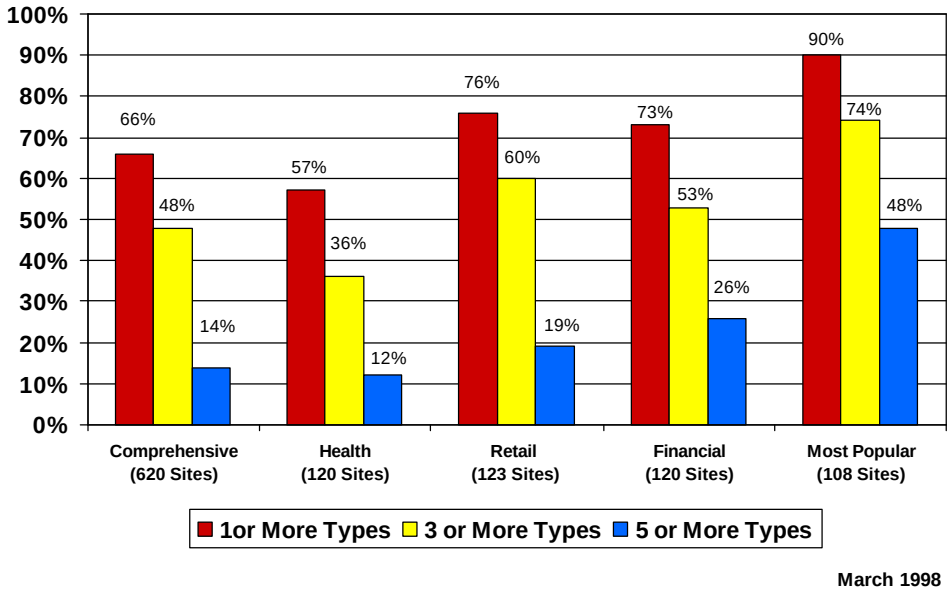


The number of sites in each sample that collect personal identifying information, such as name, e-mail or postal address, credit card number or Social Security number, is also worthy of note.[110] All of the sites in the Health, Retail, and Most Popular Samples that collect personal information, and all but one of such sites in each of the Comprehensive and Financial Samples, collect at least one item of personal identifying information.[111] All of these sites, therefore, are capable of creating personal profiles of online consumers by tying any demographic or interest information they collect to personal identifying information.[112]

Indeed, many of the sites that collect a consumer's name or e-mail address also collect other types of information about the consumer. For example, of those sites in the Comprehensive Sample that collect a consumer's name and/or e-mail address, 14% collect five or more additional types of personal information, 48% collect three or more additional types of personal information, and 66% collect at least one other type of personal information. The numbers in the Most Popular Sample are significantly higher. Of those sites in the Most Popular Sample that collect a consumer's name and/or e-mail address, 48% collect five or more additional types of personal information, 74% collect three or more additional types of personal information, and 90% collect at least one additional type of personal information.[113]

Figure 3

Of those Web Sites that Collect Name and/or E-Mail Address, Percent that Collect One or More Additional Type(s) of Personal Information, By Sample



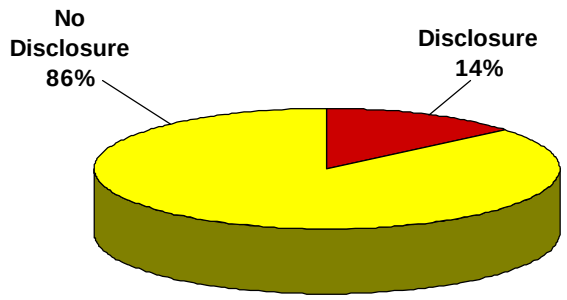
3. FREQUENCY OF DISCLOSURES

a. Random Samples

In contrast to the number of sites that collect personal information, the number of sites in the random samples that have any type of information practice disclosure, *i.e.*, either a Privacy Policy Notice or an Information Practice Statement, is extremely low. This result is consistent across all four of these samples. Only 14% of all sites in the Comprehensive Sample, 14% of all sites in the Health Sample, 13% of all sites in the Retail Sample, and 16% of all sites in the Financial Sample post any disclosure.[114]

Figure 4

Percent of Web Sites with an Information Practice Disclosure
Comprehensive Sample



Base: All Web sites in Comprehensive Sample (674) March 1998

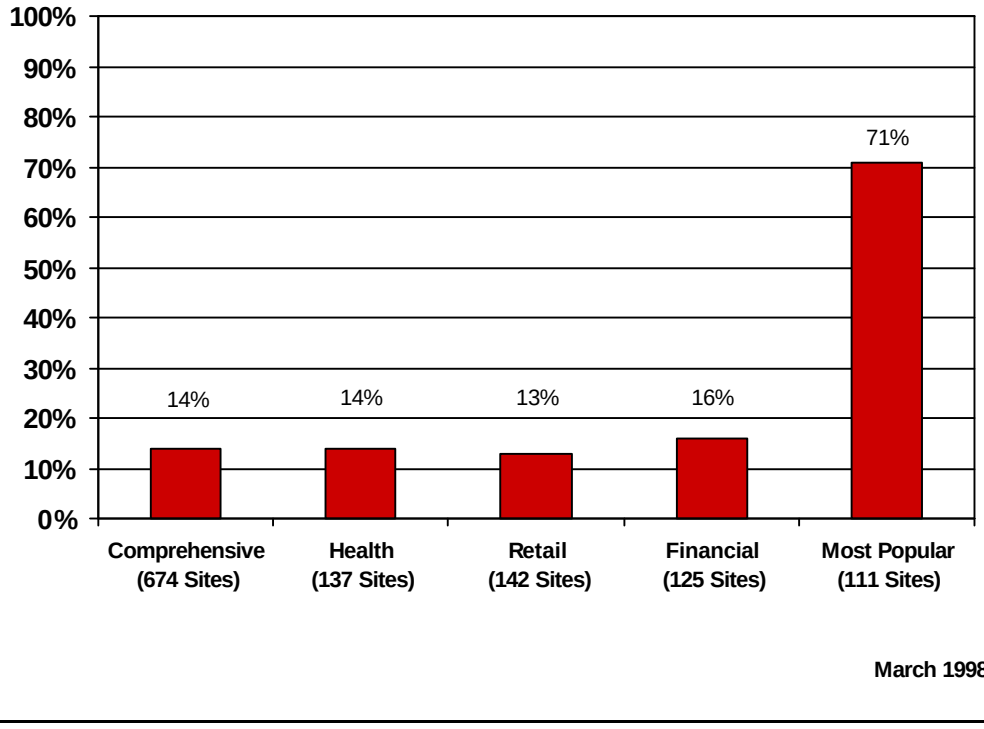
Among sites in the random samples that collect personal information, the disclosure rate is equally low. Of these sites, only 15% in the Comprehensive Sample, 16% in the Health Sample, 15% in the Retail Sample, and 17% in the Financial Sample have any information practice disclosure.[115] Only 2% of the sites that collect personal information in each of these samples have a Privacy Policy Notice.[116] Of sites that collect personal information, 14% in the Comprehensive Sample, 16% in the Health Sample, 13% in the Retail Sample, and 15% in the Financial Sample have at least one Information Practice Statement.[117]

b. Most Popular Sample

The disclosure rate is much higher in the Most Popular Sample (Sample F). Seventy-one percent of all sites have some type of information practice disclosure (either a Privacy Policy Notice or an Information Practice Statement),[118] and 73% of sites that collect personal information have such a disclosure.[119] Of the sites in this sample that collect personal information,

Figure 4A

Percent of Web Sites with an Information Practice Disclosure, By Sample

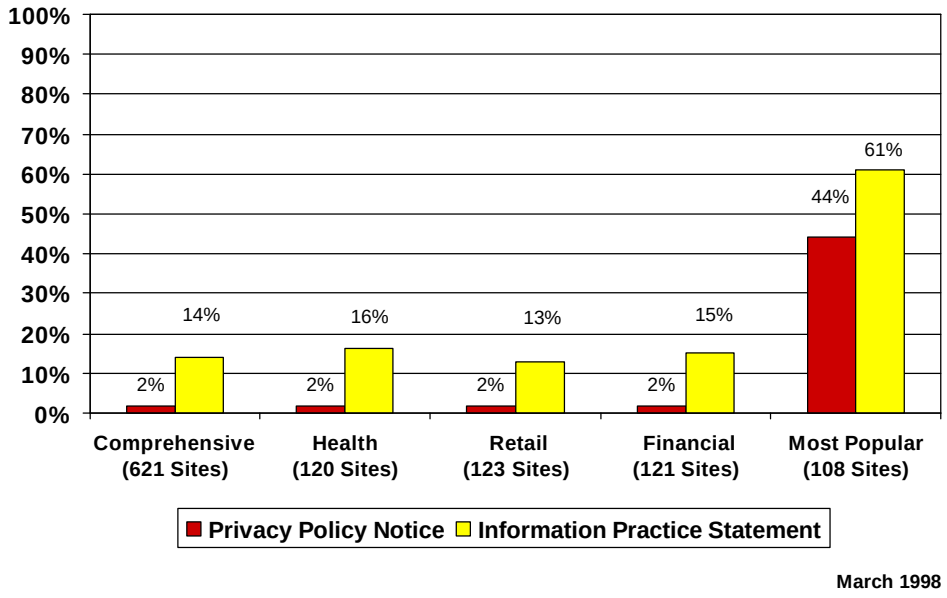


44% have a Privacy Policy Notice,[120] and 61% have at least one Information Practice Statement.[121] The higher disclosure rate for the Most Popular Sample demonstrates that providing notice to consumers is feasible. The higher disclosure rate may be attributable not only to these companies' awareness of online privacy issues, but also to the fact that, of all the sites surveyed for this report, only companies in this sample were on notice that their sites would *all* be

included in the survey, as a result of both press reports and public statements by Commission staff.[122] However, despite this clear public notice, over one-quarter of these sites still failed to post an information practice disclosure.

Figure 5

Of those Web Sites that Collect Personal Information,
Percent with a Privacy Policy Notice or
an Information Practice Statement, By Sample



4. NATURE OF DISCLOSURES

a. Random Samples

As noted above, the disclosure rate for the Comprehensive, Health, Retail, and Financial Samples is very low, ranging between 13% and 16% of all sites. The following discussion of the substance of those disclosures pertains only to those sites in each sample that both collect personal information *and* have at least one information practice disclosure: 94 sites in the Comprehensive Sample; 19 sites in the Health Sample; 18 sites in the Retail Sample; and 20 sites

in the Financial Sample.[123] The small sample size makes it difficult to draw conclusions regarding the nature of disclosures and, therefore, the analysis should be read with the small number of relevant sites in mind.[124]

Roughly one-third of the sites in each of these samples that have at least one information practice disclosure state that they give consumers choice about how the personal information they collect will be used.[125] The percent of sites offering consumers access to their personal information and/or an opportunity to correct any inaccuracies in that information is much lower, ranging from 0% in the Health and Financial Samples to 17% (or 3 sites) in the Retail Sample.[126] The percent of sites that state that they take steps to provide security for the personal information collected after they receive it ranges from 0% in the Health Sample to 15% (or 14 sites) in the Comprehensive Sample.[127]

Staff also gathered data regarding the number of sites whose disclosures address the issue of the potential transfer of personal information to third parties. The percent of sites stating that none of the personal information they collect will be disclosed to third parties ranges from 20% (or 4 sites) in the Financial Sample to 33% (or 31 sites) in the Comprehensive Sample.[128] Twenty-six percent (or 5 sites) of the sites with some information practice disclosure in the Health Sample, 33% (or 6 sites) in the Retail Sample, 36% (or 34 sites) in the Comprehensive Sample, and 40% (or 8 sites) in the Financial Sample state that at least some of the personal information collected may be released to third parties.[129] Only a single site that collects personal information in the Comprehensive Sample — and none of the sites in the other random samples — states that it provides choice, access, and security and addresses the issue of third-party disclosures.[130]

b. Most Popular Sample

The disclosure rate for the most frequently trafficked sites on the Web is, as noted above, significantly higher than the rates for the four random samples. Of the sites in this sample that both collect personal information and have at least one information practice disclosure, 68% (or 54 sites) state that they give consumers choice about how the personal information collected will be used,[131] 38% (or 30 sites) state that they provide consumers access to their personal information and/or an opportunity to correct any inaccuracies in that information,[132] and 16% (or

13 sites) state that they take steps to provide security for the personal information collected after they receive it.[133]

Fourteen percent (or 11 sites) of the sites in this sample that collect personal information and have an information practice disclosure say that none of the personal information they collect will be disclosed to third parties.[134] Seventy-eight percent (or 62 sites) of these sites state that at least some of the personal information collected may be released to third parties.[135] Six percent (or 5 sites) of these sites say that they provide consumers choice, access, and security, and address the issue of third-party disclosures.[136]

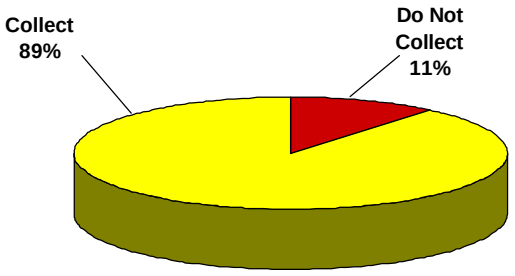
C. CHILDREN'S SURVEY FINDINGS

1. PERSONAL INFORMATION COLLECTION FROM CHILDREN

Commission staff surveyed Web sites in this Sample to ascertain whether they collect personal information from children online, and, if so, to identify the types of information they collect. Staff found that 89% of the 212 sites collect one or more types of personal information from children (a rate comparable to all of the other samples)[137] and that 88% collect at least one type of personal identifying information as well.[138] Personal information collected from children includes a wide array of identifying information such as name, e-mail address,[139] postal address,

Figure 6

Percent of Web Sites Collecting Personal Information from Children

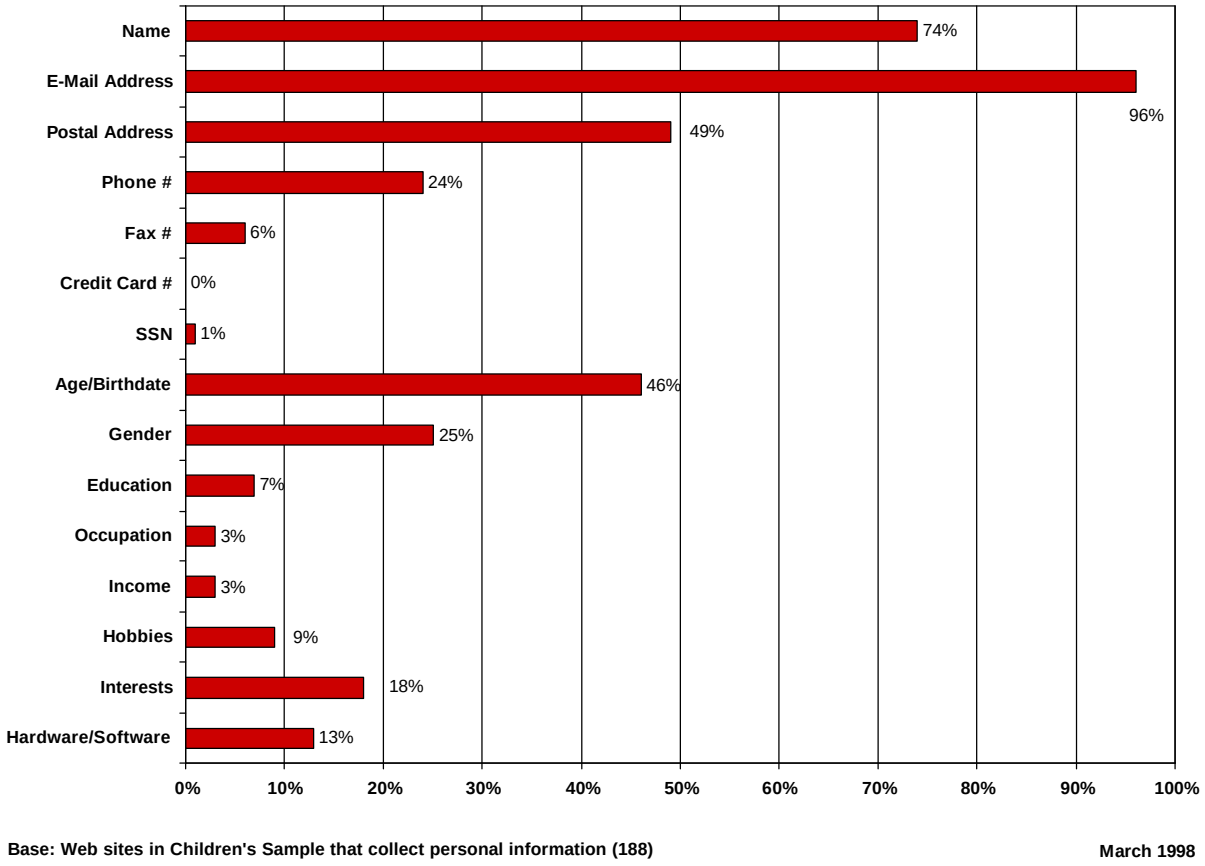


Base: All Web sites in Children's Sample (212) March 1998

telephone number, and Social Security number, as well as other personal information like age or date of birth, gender, education, interests, and hobbies.[140]

Figure 7

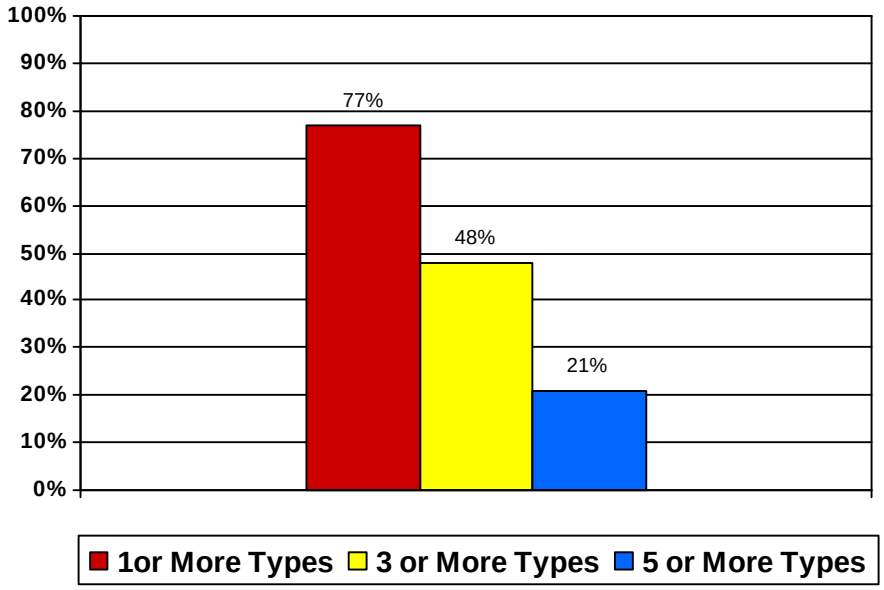
Types of Personal Information Collected from Children



Often the sites that collect personal identifying information also collect several other types of information, enabling them to form a detailed profile of a child. In fact, of the sites that collect a child's name and/or e-mail address, 21% collect five or more additional types of personal information, 48% collect three or more additional types of personal information, and 77% collect one or more additional types of personal information from children.[141]

Figure 8

Of those Web Sites that Collect Name and/or E-Mail Address,
Percent that Collect One or More Additional
Type(s) of Personal Information from Children



Base: Web sites in Children's Sample that collect name and/or e-mail address from children (186) **March 1998**

Web sites use a variety of techniques to solicit personal information from children. For example, some sites require children to answer questions about their interests in order to register or to become eligible to win prizes.[142] In other cases a site may use "imaginary" characters to request information from children, have children sign a "guest book," solicit information to create home pages for children, invite children to participate in chat and electronic pen pal programs, require children to register with the site for updates and information, and offer prizes and other incentives for completing surveys and polls. Some sites use detailed questionnaires, soliciting information about children's age, gender, geographic location, and even personal finances.[143]

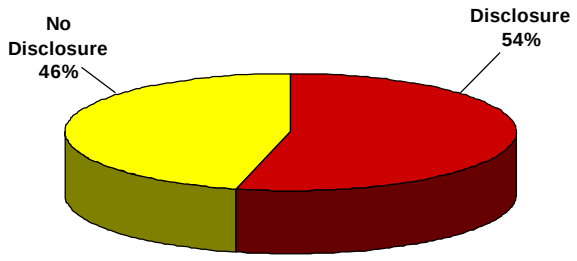
While it was not possible to determine all the purposes for which personal information collected from children is used, many uses were apparent simply from visiting sites. Surfers found, for example, that some sites collect e-mail addresses to send children newsletters and notices about online contests and chances to win prizes on the site. Other sites collect personal information from children to notify them of contest results and to ask children for feedback about the site.

2. FREQUENCY OF DISCLOSURES

The percentage of children's sites providing some degree of disclosure about their collection and use of information was significantly higher than that for all samples other than the Most Popular Sample.[144] Fifty-four percent of all sites in the Children's Sample have some kind of information practice disclosure, either a comprehensive Privacy Policy Notice or at least one Information Practice Statement, or both.[145]

Figure 9

Percent of Children's Web Sites
with an Information Practice Disclosure



Base: All Web sites in Children's Sample (212) March 1998

As noted above with respect to the general samples, staff applied a very broad definition of what constitutes an Information Practice Statement. Any statement that describes a particular use or practice regarding consumers' personal information and/or a choice offered to consumers about their personal information was considered an Information Practice Statement. Examples from the Children's Sample include statements such as:

- Kids, get your parents' permission before you give out information online;
- We reserve the right to do whatever we want with the information we collect, and

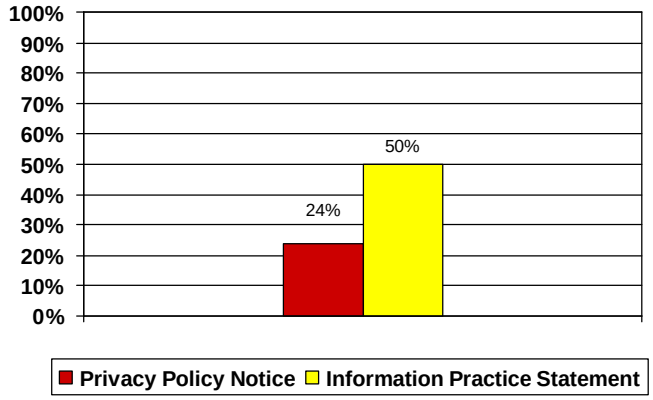
C Click here if you want to be on our mailing list.

Of sites that collect personal information from children, 50% have at least one Information Practice Statement.[146]

Although a majority of children's sites have some statement about one or more of their information practice(s), the number of children's sites that have a Privacy Policy Notice is much lower. Twenty-four percent of the sites that collect personal information from children post a Privacy Policy Notice.[147]

Figure 10

Of those Web Sites that Collect Personal Information from Children, Percent with a Privacy Policy Notice or an Information Practice Statement



Base: Web sites in Children's Sample that collect personal information (188)

March 1998

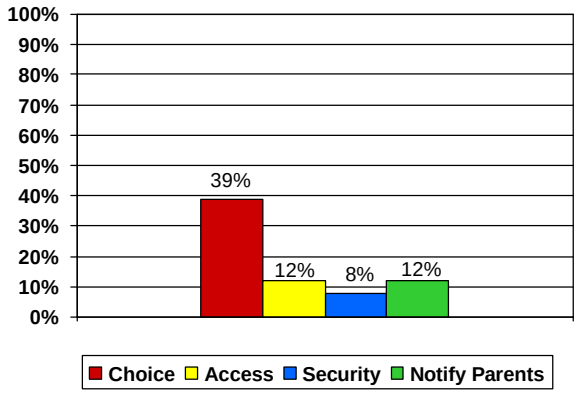
3. NATURE OF DISCLOSURES

The following discussion of the nature of disclosures by sites in the Children's Sample applies only to those sites that both collect personal information from children and have at least one information practice disclosure (109 sites). Thirty-nine percent (or 43 sites) of these sites say

that they provide children or their parents with choices about how their personal information will be used.[148] Only 12% (or 13 sites) of these sites say that they offer access to this personal information or an opportunity to correct inaccuracies.[149] The percentage of sites that state they take steps to provide security for personal information after they receive it is lower still — 8% (or 9 sites).[150] Only 12% (or 13 sites) say they will notify parents of their information practices. Of the sites that collect personal information from children and have at least one information practice disclosure, no site's information practice disclosure discusses the full range of fair information practice principles — choice, access, security *and* parental notice.

Figure 11

Of those Sites that Collect Personal Information from Children and Have an Information Practice Disclosure, Percent that Offer Choice, Access, Security and/or Notify Parents of Information Practices



Base: Web sites in Children's Sample that collect personal information from children and have an Information Practice Disclosure (109)

March 1998

The survey also shows that numerous sites disclose children's personal information to third parties. There are two ways that sites disclose personal information to third parties: (1) sites may display children's personal information in areas accessible to anyone online; or (2) sites may sell or rent children's personal information to others. In either case, the release of children's personal

identifying information to third parties is of concern, because it creates a risk of injury to or exploitation of children so identified. As described earlier, 97% of parents are concerned about whether their children's personal information is shared with third parties.[151] Despite parents' concern, staff found sites, for example, that display color photographs of young children with their full names and ages, as well as sites that facilitate public disclosure of children's e-mail addresses in bulletin boards, chat rooms, "art galleries," and on children's home pages.

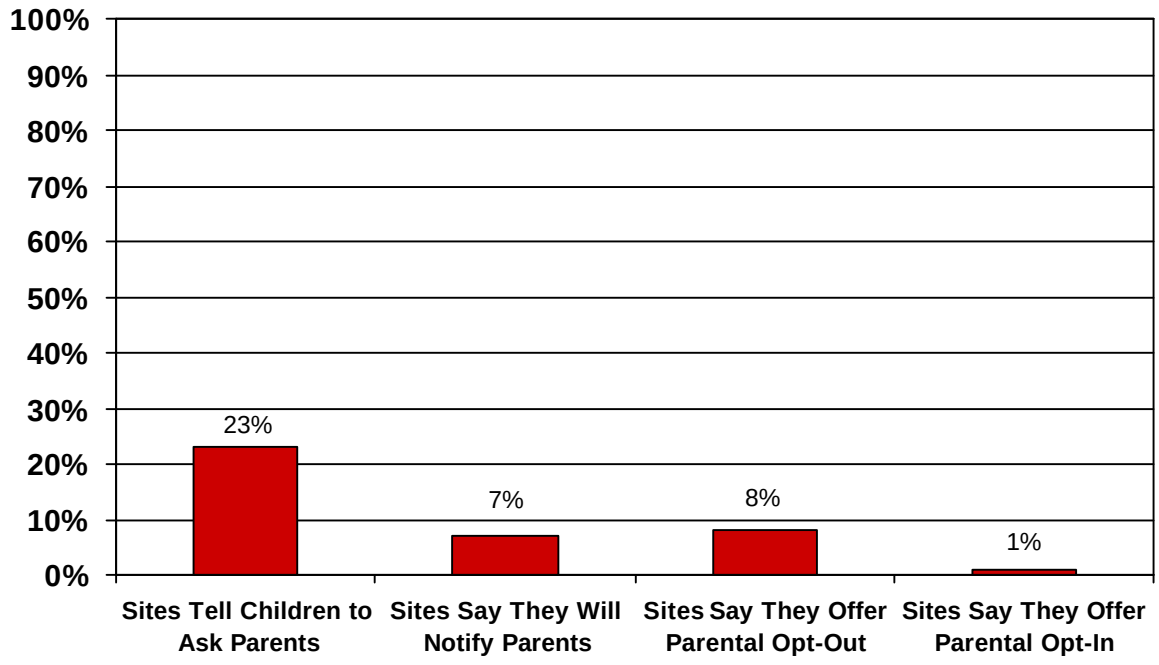
Of those sites that collect personal information from children and have an information practice disclosure, 82% have some kind of disclosure stating whether or not children's information will be publicly posted or otherwise shared with third parties.[152] Only 33% have an information practice disclosure stating that *none* of the information will be released to third parties.[153] Forty-nine percent say that the information *may* be released to third parties.[154]

4. PARENTAL INVOLVEMENT

The role of parents in protecting their children's privacy is fundamental to the implementation of the fair information practice principles described in this report, and is the principle touchstone of both the staff opinion letter and the CARU guidelines. The survey percentages were low with regard to parental control over the collection and use of information. Only 23% (or 48 sites) of all the sites in the Children's Sample take the first step of telling children to ask their parents for permission before providing information to the site.[155] Less than 8% of the sites say they notify parents of their information practices.[156] Only 1% (or 3 sites) require parental consent to the collection and use of information *before* the information is collected or used (opt-in)[157] and only 8% (or 17 sites) say that parents can ask that personal information collected from children be deleted or not used in the future (opt-out).[158]

Figure 12

Percent of Web Sites with Disclosures
Regarding Parental Involvement



Base: All Web sites in Children's Sample (212) **March 1998**

The results reveal a very low level of compliance with the basic parental control principles contained in the staff opinion letter and the CARU guidelines more than seven months after these documents were released. First, the results demonstrate that a significant percentage of sites continue to collect a vast array of personal information from children, in sharp contrast to parents' preferences.[159] Second, despite the fact that Commission staff publicly disclosed that the Children's Sample would be selected from sites listed in the Yahooligans! Directory, nearly half of the sample failed to post any kind of information practice disclosure. Finally, very few sites tell children to ask their parents for permission before providing personal information, and fewer still notify parents of their information practices or appear to take any steps to involve parents.

VI. CONCLUSIONS

- A medical clinic's online doctor-referral service invites consumers to submit their name, postal address, e-mail address, insurance company, any comments concerning their medical problems, and to indicate whether they wish to receive information on any of a number of topics, including urinary incontinence, hypertension, cholesterol, prostate cancer, and diabetes. The online application for the clinic's health education membership program asks consumers to submit their name, address, telephone number, date of birth, marital status, gender, insurance company, and the date and location of their last hospitalization. The clinic's Web site says nothing about how the information consumers provide will be used or whether it will be made available to third parties.

- An automobile dealership's Web site offers help to consumers in rebuilding their credit ratings. To take advantage of this offer, consumers are urged to provide their name, address, Social Security number, and telephone number through the Web site's online information form. The Web site says nothing about how the information provided will be used or whether it will be made available to third parties.

- A mortgage company operates an online prequalification service for home loans. The online application form requires that each potential borrower provide his or her name, Social Security number, home and business telephone numbers, e-mail address, previous address, type of loan sought, current and former employer's name and address, length of employment, income, sources of funds to be applied toward closing, and approximate total in savings. The online form also requires the borrower to provide information about his or her credit history, including credit card, car loans, child support and other indebtedness, and to state whether he or she has ever filed for bankruptcy. The application form requires the borrower to agree that the mortgage company may disclose his or her "credit experiences" to third parties, but the Web site says nothing else about how the mortgage company might use all of the information provided or whether that information will be made available to third parties.

- A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The Web site also asks a child extensive personal finance questions, such as whether a child has received gifts in the form of stocks, cash, savings bonds, mutual funds, or certificates of deposit; who has given a child these gifts; whether a child puts monetary gifts into mutual funds, stocks or bonds; and whether a child's parents own mutual funds. Elsewhere on the Web site, contest winners' full names, age, city, state, and zip code are posted. The Web site does not tell children to ask their parents for permission before providing personal

information and does not appear to take any steps to involve parents. Further, the Web site says nothing about whether the information is disclosed to third parties.

- Another child-directed site collects personal information to register for a chat room, including a child's full name, e-mail address, city, state, gender, age, and hobbies. The Web site has a lotto contest that asks for a child's full name and e-mail address. Lotto contest winners' full names are posted on the site. For children who wish to find an electronic pen pal, the site offers a bulletin board service that posts messages, including children's e-mail addresses. While the Web site says it asks *children* to post messages if they are looking for a pen pal, in fact, anyone of any age can visit this bulletin board and contact a child directly. The site also has an area where children can submit stories online. The Web site posts the stories along with children's full names, ages, and e-mail addresses. The Web site does not tell children to ask their parents for permission before providing personal information and does not say that it takes steps to involve parents. The Web site says nothing about whether the information is disclosed to third parties.

* * *

The practices of these Web sites demonstrate the real need for implementing the basic fair information practices described in this report. The World Wide Web provides a host of opportunities for businesses to gather a vast array of personal information from and about consumers, including children. The online environment and the advent of the computer age also provide unprecedented opportunities for the compilation, analysis, and dissemination of such information. While American businesses have always collected some information from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns.

The federal government currently has limited authority over the collection and dissemination of personal data collected online.[160] The Federal Trade Commission Act (the "FTC Act" or "Act")[161] prohibits unfair and deceptive practices in and affecting commerce. The Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of

the Act, and provides a basis for government enforcement of certain fair information practices. For instance, failure to comply with stated information practices may constitute a deceptive practice in certain circumstances, and the Commission would have authority to pursue the remedies available under the Act for such violations. Furthermore, in certain circumstances, information practices may be inherently deceptive or unfair, regardless of whether the entity has publicly adopted any fair information practice policies. As discussed above, Commission staff has issued an opinion letter addressing the possible unfairness inherent in collecting certain personal identifying information from children online and transferring it to third parties without obtaining *prior* parental consent.[162] However, as a general matter, the Commission lacks authority to require firms to adopt information practice policies.

The Commission has encouraged industry to address consumer concerns regarding online privacy through self-regulation. The Internet is a rapidly changing marketplace. Effective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy. Accordingly, a private-sector response to consumer concerns that incorporates widely-accepted fair information practices and provides for effective enforcement mechanisms could afford consumers adequate privacy protection. To date, however, the Commission has not seen an effective self-regulatory system emerge.

As evidenced by the Commission's survey results, and despite the Commission's three-year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness). Moreover, the trade association guidelines submitted to the Commission do not reflect industry acceptance of the basic fair information practice principles. In addition, the guidelines, with limited exception, contain none of the enforcement mechanisms needed for an effective self-regulatory regime. In light of the lack of notice regarding information practices on the World Wide Web and the lack of current industry guidelines adequate to establish an effective self-regulatory regime, the question is what additional incentives are required in order to encourage effective self-regulatory efforts by industry. The Commission currently is

considering this question in light of the survey results, monitoring self-regulation efforts since the survey was completed, and assessing the utility and effectiveness of different courses of action. This summer, the Commission will make recommendations on actions it deems necessary to protect online consumers generally.

In the specific area of children's online privacy, however, the Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children. Such legislation would set out the basic standards of practice governing the online collection and use of information from children. All commercial Web sites directed to children would be required to comply with these standards.

In making this recommendation, the Commission has drawn on its extensive experience in addressing business practices affecting children, as well as its three-year study of online privacy issues. The Commission has already taken some steps, particularly the release of the staff opinion letter, to address online information practices involving children that may violate Section 5 of the Federal Trade Commission Act. Moreover, the Commission has recognized a growing consensus reflected in consumer survey evidence and some industry self-regulatory guidelines that parental involvement is necessary in the collection and use of information from children. Nonetheless, Section 5 may only have application to some but not all of the practices that raise concern about the online collection and use of information from children. The Commission does not believe, for example, that Section 5 necessarily authorizes it to require parental notice and involvement across the board for all commercial Web sites engaged in information collection from children. Accordingly, the Commission concludes that as a matter of policy additional steps should now be taken to ensure adequate online privacy protections for children.

Children's privacy legislation also would recognize that a marketer's responsibilities vary with the age of the child from whom personal information is sought. In a commercial context, Congress and industry self-regulatory bodies traditionally have distinguished between children aged 12 and under, who are particularly vulnerable to overreaching by marketers, and children over the age of 12, for whom strong, but more flexible protections may be appropriate. In each

case, the goal of legislative requirements should be to recognize the parents' role with respect to information collection from children.

Accordingly, the Commission recommends that Congress develop legislation to require commercial Web sites that collect personal identifying information from children 12 and under to provide actual notice to the parent and obtain parental consent as follows:

- Where the personal identifying information would enable someone to contact a child **offline**, the company must obtain *prior parental consent*, regardless of the intended use of the information (opt-in);
- Where the personal identifying information is **publicly posted or disclosed to third parties**, the company must obtain *prior parental consent* (opt-in)*;*
- Where collection of an e-mail address is necessary for a child's participation at a site, such as to notify contest winners, the company must provide *notice* to parents and an opportunity to remove the e-mail address from the site's database (opt-out).

Where the personal identifying information is collected from children over 12, the Commission recommends that:

- Web sites must provide parents with notice of the collection of such information and an opportunity to remove the information from the site's database (opt-out).[163]

The development of the online marketplace is at a critical juncture. If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential. To date, industry has had only limited success in implementing fair information practices and adopting self-regulatory regimes with respect to the online collection, use, and dissemination of personal information. Accordingly, the Commission now recommends legislation to protect children online and this summer will recommend an appropriate response to protect the privacy of all online consumers.

ENDNOTES

1. In July 1997 the Commission promised that it would submit this report in June 1998. Commission letter to Senator John McCain, Chairman, Committee on Commerce, Science and Transportation, United States Senate (July 31, 1997); Commission Letter to Representative Thomas Bliley, Chairman, Committee on Commerce, United States House of Representatives (July 31, 1997) (hereinafter referred to as "McCain/Bliley letters"). The text of the McCain/Bliley letters may be found on the Commission's Web site at http://www.ftc.gov/os/9707/privac97.htm.

2. The Commission's Public Workshop on Consumer Information Privacy ("1997 Workshop"), June 10-13, 1997, also explored the privacy issues raised by computerized databases that contain consumers' personal identifying information (also known as "individual reference services" or "look-up" services), as well as issues relating to unsolicited commercial e-mail. The workshop transcript may be found on the Commission's Web site at http://www.ftc.gov/bcp/privacy/wkshp97/index.html.

3. These Commission efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. The Commission and its staff have also issued reports describing various consumer privacy concerns in the electronic marketplace. *E.g.*, FTC Report to Congress: *Individual Reference Services*, December 1997, available on the Commission's Web site at http://www.ftc.gov/bcp/privacy/wkshp97/index.html [hereinafter "*FTC Report to Congress/Reference Services*"]; FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996, available at http://www.ftc.gov/reports/privacy/privacy1.htm [hereinafter "*FTC Staff Report*"]; FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, May 1996, available at http://www.ftc.gov/opp/global.htm. In addition, the Commission presented testimony on the Implications of Emerging Electronic Payment Systems on Individual Privacy on September 18, 1997 before the House Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services (available at http://www.ftc.gov/os/9709/elecpay.tes.htm); and on Internet Privacy on March 26, 1998 before the House Subcommittee on Courts and Intellectual Property, Committee on the Judiciary (available at http://www.ftc.gov/os/9803/privacy.htm).

4. "Cookie" technology allows a Web site's server to place information about a consumer's visits to the site on the consumer's computer in a text file that only the Web site's server can read. Using cookies a Web site assigns each consumer a unique identifier (not the actual identity of the consumer), so that the consumer may be recognized in subsequent visits to the site. On each return visit, the site can call up user-specific information, which could include the consumer's preferences or interests, as indicated by documents the consumer accessed in prior visits or items

the consumer clicked on while in the site. Web sites can also collect information about consumers through hidden electronic navigational software that captures information about site visits, including Web pages visited and information downloaded, the types of browser used, and the referring Web sites' Internet addresses. Staff did not ascertain whether sites in the Commission's online survey use cookies, or other hidden electronic means, to collect personal information, but looked instead to sites' information practice disclosures to reveal such practices. *See infra* Section V.A and Appendix A.

5. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old), available at http://www.commerce.net/work/pilot/nielsen_96/press_97.html [hereinafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS ™): Second Quarter 1997 Study* (Sept. 4, 1997), available at http://www.intelliquest.com/about/release32.htm.

6. *CommerceNet/Nielsen Demographic Study*, Spring '97.

7. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997), available at http://www.commerce.net/news/press/121197.html [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. *See also* Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (finding that 23% of users ordered and paid for a product over the Internet, *i.e.*, "transacted" business online), available at http://www.yankelovich.com/pr/970327.htm.

8. Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (figure includes directory listings and classified advertisements), available at http://www.jup.com/digest/082297/advert.shtml.

9. Louis Harris & Associates and Dr. Alan F. Westin, *Commerce, Communication, and Privacy Online, A National Survey of Computer Users* (1997) (hereinafter referred to as "*Westin Survey*") at ix.

The Commission recognizes that the widespread availability of consumers' personal information, and the privacy concerns raised thereby, are not unique to the Internet. The Commission has focussed on online privacy for several reasons. First, interactive media make it possible to collect, store, aggregate, and disseminate personal information with speed and efficiency that are unmatched in other contexts. Second, the fact that the online marketplace is in its infancy makes it possible to address online privacy issues prospectively. Finally, and most important, consumers' concerns about their privacy are significantly heightened in the online environment.

10. *Id.* at 20-21.

11. *Business Week/Harris Poll: Online Insecurity*, Business Week, March 16, 1998, at 102.

12. Privacy & American Business Report, Vol. 4, No. 3 (1997) (reporting on Louis Harris Associates and Alan F. Westin's *National Survey of Computer Users*).

13. As the Commission's expertise and regulatory authority relate to commercial activities, its review of children's online privacy issues has focused on the information practices of commercial Web sites. The collection of information from and about children by non-commercial sites such as those operated by non-profit and educational entities, however, raises similar privacy concerns.

14. Interactive Consumers Research Report, Vol. 4, No. 5 at 1, 4, May 1997 (discussing results of FIND/SVP's 1997 American Internet User Survey).

15. *Id*. at 3. The Find/SVP's survey regarding children's online activities reports that approximately 57% of households with online children use the Internet for homework and school-related research (64% with children ages 8 to 11); 51% use it for entertainment or games (78% with children ages 8 to 11); 45% use it for surfing or browsing (60% with children ages 8 to 11); 37% use it for e-mail and chat (35% with children ages 8 to 11); and 43% use it for informal learning (59% with children ages 8 to 11).

16. *Id*. at 1, 2. The number of children online increased nearly five-fold from fall 1995 to spring 1997. *Id.* at 1.

17. One source has estimated that, in 1997, children aged 4 through 12 spent $24.4 billion themselves; and children aged 2 through 14 may have directly influenced spending by their parents in an amount as much as $188 billion. James U. McNeal, *Tapping the Three Kids' Markets*, American Demographics, Apr. 1998, at 38, 40.

18. According to one source, most children's Web sites are targeting children ages 8 to 11. Teens tend to visit the same sites that adults visit. Robin Raskin, *What do Kids Want?*, Family PC Magazine, May 1998, at 17.

19. The types of personal information include personal identifying information, such as name, e-mail address, phone number, and home address, as well as other personal information such as the child's age, gender, hobbies, interests, favorite foods, games, movies, books, and animated characters. *See infra* Section V. C. 1.

20. *See FTC Staff Report*, Appendix E.

21. The "Innocent Images" program focuses on individuals who go online to meet children for the purpose of engaging in sexual activity or who produce and/or distribute child pornography online. *See* 1997 Workshop, Transcript at 229 (testimony of FBI agent Linda Hooper). *See also* Testimony of Louis J. Freeh, Director, Federal Bureau of Investigation, before the Senate

Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 10, 1998, available at http://www.fbi.gov/congress/internet/sac310.htm; and Testimony of Stephen R. Wiley, Chief, FBI Violent Crime and Major Offenders Section, before the House Subcommittee on Crime, Committee on the Judiciary, November 7, 1997, available at http://www.fbi.gov/congress/children/children.htm.

22. 1997 Workshop, Transcript at 192-93 (testimony of Charlotte Baecher of Consumers Union).

23. *Id.* at 36-37.

24. *Id.*

25. *Id.*

26. *Id.* at 156 (testimony of Alan Westin).

27. Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens* (1973) [hereinafter "HEW Report"]. In the twenty-five years that have elapsed since the HEW Report, a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) [hereinafter "*Privacy Protection Study*"]; Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) [hereinafter "*OECD Guidelines*"]; Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995) [hereinafter "*IITF Report*"]; U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995) [hereinafter "*Commerce Report*"]; *The European Union Directive on the Protection of Personal Data* (1995) [hereinafter "*EU Directive*"]; and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996) [hereinafter "*CSA Model Code*"]. Other sources relied upon herein include the *FTC Staff Report* and *FTC Report to Congress/Reference Services.*

28. Such principles can be either procedural or substantive. Procedural principles address how personal information is collected and used by governing the methods by which data collectors and data providers interact. These principles ensure that consumers have notice of, and consent to, an entity's information practices. Substantive principles, by contrast, impose substantive limitations on the collection and use of personal information, regardless of consumer consent, by requiring

that only certain information be collected and that such information only be used in certain ways. Most of the principles discussed below are procedural in nature. One substantive principle widely adopted by the fair information practice codes, but not discussed below, is the collection limitation principle, which states that entities should only collect personal information necessary for a legitimate business purpose. *See Privacy Protection Study* at 513-15; *IITF Report* § II.A; *CSA Model Code* ¶ 4.4.

29. *See, e.g.*, *OECD Guidelines, Explanatory Memorandum* ¶ 52; *see also FTC Staff Report* at 9.

30. While notice of a Web site's policies with respect to data integrity and security is critical to making an informed decision to reveal personal data, such notice is not a prerequisite to the implementation of security measures. The implementation of security measures lies solely in the hands of the entity collecting the information and requires no active participation from the consumer. Implementation of the principles of choice and access, by contrast, require consumer involvement and, therefore, are dependent on notice to be meaningful.

31. *OECD Guidelines*, Openness Principle & ¶ 12; *FTC Staff Report* at 9-10; *EU Directive* art. 10; *CSA Model Code* ¶ 4.8.2.

32. *HEW Report* at 62; *Privacy Protection Study* at 514; *OECD Guidelines*, Purpose Specification Principle & ¶ 9; *IITF Report* § II.B.; *Commerce Report* at 21; *EU Directive* art. 10; *CSA Model Code* ¶ 4.2; *FTC Staff Report* at 9-10. The corollary to identifying the purposes for data collection is that the data not be used for other purposes without the data subject's consent. *See HEW Report* at 61-62; *OECD Guidelines*, Use Limitation Principle & ¶ 10 and *Explanatory Memorandum* ¶ 55; *IITF Report* § II.D; *EU Directive* arts. 6-7; *CSA Model Code* ¶ 4.5.

33. *EU Directive* art. 10.

34. *Commerce Report* at 21.

35. *HEW Report* at 59; *IITF Report* § II.B; *EU Directive* art. 10. Several of the fair information practice codes recognize that a consumer's refusal to allow the further unrelated use of his or her personal information, beyond that which is necessary to complete the transaction at issue, should not form the basis for the denial of access to the good or service in question. *See, e.g.*, *Commerce Report* at 25; *CSA Model Code* ¶ 4.3.3.

36. *Privacy Protection Study* at 514; *IITF Report* § II.B. As noted in endnote 30, notice of this type is not a prerequisite to insuring the confidentiality, integrity, and quality of data. However, when dealing with data considered by consumers to be particularly sensitive, information about the steps taken by the data collector is important to the consumer and may determine whether the consumer is willing to provide such data.

37. *See FTC Staff Report* at 9-10.

38. *HEW Report* at 58; *CSA Model Code* ¶ 4.8.2; *EU Directive* art. 10.

39. *HEW Report* at 58; *EU Directive* art. 10.

40. *IITF Report* § II.B.

41. *Cf. CSA Model Code* ¶ 4.8.2 (organizations should make available identity of individual accountable for organization's policies and to whom complaints can be forwarded).

42. Virtually every set of fair information practice principles includes consumer choice or consent as an essential element. *HEW Report* at 41, 61; *OECD Guidelines*, Collection Limitation Principle & ¶ 7 and Use Limitation Principle & ¶ 10; *Commerce Report* at 23-27; *EU Directive* arts. 7, 14; *CSA Model Code*, ¶¶ 4.3, 4.5; *see also FTC Report to Congress/Reference Services* at 22-23; *FTC Staff Report* at 10-11.

43. As noted in the FTC Staff Report, commentators have taken different views of the efficacy and wisdom of opt-in versus opt-out regimes. *FTC Staff Report* at 10-11; *see also Commerce Report* at 24-27 (proposing opt-in regimes for "sensitive information" and opt-out regimes for other information).

44. Indeed, technological innovations soon may allow consumers and collectors of information to engage in "electronic negotiation" regarding the scope of information disclosure and use. Such "negotiation" would be based on electronic matching of pre-programmed consumer preferences with Web sites' information practices. The World Wide Web Consortium ("W3C") is currently in the final stages of developing its Platform for Privacy Preferences Project ("P3P"), which will allow implementation of such technology. Consumers may have access to P3P by early 1999. For general information on P3P, see the W3C's Web site (http://www.w3.org/P3P).

45. A system requiring consumers to specify privacy preferences before visiting any Web sites can be built into Internet browsers. *See supra* note 44 (discussing technological developments). The absence of default rules, and the concomitant requirement that consumers decide how they want their personal information used, help ensure that consumers in fact exercise choice.

46. *See HEW Report* at 41, 59, 63; *Privacy Protection Study* at 508-13; *OECD Guidelines*, Individual Participation Principle & ¶ 13; *IITF Report* § III.B; EU Directive art. 12; *CSA Model Code* ¶ 4.9; *FTC Report to Congress/Reference Services* at 21-22. *See also* Fair Credit Reporting Act ("FCRA") §§ 609-11, 15 U.S.C. §§ 1681g-1681i (providing for consumer access to, and the right to correct inaccuracies in, consumer credit reports).

47. *See HEW Report* at 63; *IITF Report* § III.B; *CSA Model Code* ¶ 4.9; *OECD Guidelines*, Individual Participation Principle & ¶ 13 and *Explanatory Memorandum* ¶ 61; *EU Directive* art. 12; *see also FTC Report to Congress/Reference Services* at 21-22; FCRA § 611, 15 U.S.C. § 1681i.

48. *HEW Report* at 56-57; *Privacy Protection Study* at 521; *OECD Guidelines*, Data Quality Principle & ¶ 8 and *Explanatory Memorandum* ¶ 53; *IITF Report* § I.C; *EU Directive* art. 6; *CSA Model Code* ¶¶ 4.5.3, 4.6; *see also* FCRA §§ 605, 607(b), 15 U.S.C. §§ 1681c, 1681e(b).

49. *OECD Guidelines*, Security Safeguards Principle & ¶ 11 and Explanatory Memorandum ¶ 56; *IITF Report* §§ I.B, II.C; *EU Directive* art. 17; CSA Model Code ¶ 4.7; *FTC Staff Report* at 12. Physical security measures, such as guards, alarms, etc., may also be necessary in certain circumstances.

50. In implementing security measures, companies should be aware that security breaches directed at *stored* data — *i.e.*, information already received by the data collector — often constitute greater threats to privacy than those breaches occurring during the *transmission* of sensitive data, such as credit card numbers, over the Internet. *See, e.g.*, Linda Punch, *The Real Internet Security Issue*, Credit Card Management, Dec. 1997, at 65.

51. *See HEW Report* at 50 (calling for Code of Fair Information Practices that includes civil and criminal penalties, the availability of injunctive relief, and individual rights of action for actual, liquidated, and punitive damages); *OECD Guidelines*, Accountability Principle & ¶14 and *Explanatory Memorandum* ¶ 62 (accountability supported by legal sanctions); *IITF Report* § III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); *EU Directive* arts. 22-23 (judicial remedy and compensation).

52. *Cf. Privacy Protection Study* at 33 (identifying voluntary compliance, statutorily-created rights enforceable through individual or government action, and centralized government mechanisms as means of implementing compliance).

53. The European Union ("EU") has recognized that self-regulation may in certain circumstances constitute "adequate" privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking "adequate" safeguards. *See EU Directive* art. 25. The EU has noted, however, that non-legal rules such as industry association guidelines are relevant to the "adequacy" determination only to the extent they are complied with and that compliance levels, in turn, are directly related to the availability of sanctions and/or external verification of compliance. *See* European Commission, Directorate General XV, *Working Document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?* (1998) available at http://www.europa.eu.int/comm/dg15/en/media/dataprot/wp7.htm [hereinafter "*Judging Industry Self-Regulation*"].

54. *Discussion Draft: Elements of Effective Self-Regulation for Protection of Privacy* (1998) available at http://www.ecommerce.gov/staff.htm [hereinafter "*Elements of Effective Self-Regulation*"] (identifying consumer recourse, verification, and consequences as elements of an effective self-regulatory regime).

55. *Id*. Commission staff recently responded to a request from the Direct Marketing Association ("DMA") for an advisory opinion concerning whether the antitrust laws would permit it to require three things of its members: (1) to use the DMA's Mail Preference and Telephone Preference Services to honor consumers' requests to not be contacted by direct marketers; (2) to disclose to consumers how members sell or otherwise transfer personal information about those consumers to others; and (3) to honor consumers' requests that the members not sell or transfer their personal information. FTC Bureau of Competition staff advised the DMA of its conclusion that these requirements, as the DMA described them, would not harm competition or violate the FTC Act. Letter from Bureau of Competition Assistant Director to Counsel for the DMA, Sept. 9, 1997, available at http://www.ftc.gov/os/9710/dma.htm.

56. *See Elements of Effective Self-Regulation*.

57. *FTC Report to Congress/Reference Services* at 25-33. It is still too early to assess the success or efficacy of this plan, because its provisions are not mandatory on its signatories until the end of the year.

58. There may, alternatively, be a role for mechanisms to address practices affecting consumers as a group, such as industry or trade association ethics or screening committees that can resolve broader disputes.

59. *See Elements of Effective Self-Regulation*.

60. Several fair information practice codes suggest compensation for injuries as an important element of fair information practice. *See HEW Report* at 50 (calling for Code of Fair Information Practices that provides for actual, liquidated, and punitive damages); *OECD Guidelines*, Accountability Principle & ¶ 14 and *Explanatory Memorandum* ¶ 62 (accountability supported by legal sanctions); *IITF Report* § III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); *see also Judging Industry Self-Regulation* at 5.

61. *HEW Report* at 50 (calling for Code of Fair Information Practices that includes civil and criminal penalties, the availability of injunctive relief, and individual rights of action for actual, liquidated, and punitive damages); *OECD Guidelines*, Accountability Principle & ¶ 14 and *Explanatory Memorandum* ¶ 62 (accountability supported by legal sanctions); *IITF Report* § III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); *EU Directive* arts. 22-23 (judicial remedy and compensation).

62. Two sectoral privacy acts provide for the recovery of actual, liquidated, and punitive damages for violations. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(c) (providing for award of actual damages or liquidated damages of not less than $2,500, punitive damages, attorney's fees, and equitable relief); Cable Communications Policy Act of 1984, 47 U.S.C.

§ 551(f) (providing for recovery of actual damages or liquidated damages of not less than $1,000, punitive damages, and attorney's fees).

63. *HEW* Report at 50; *IITF Report* § III.C (discussing regulatory enforcement and criminal prosecution as redress options); *OECD Guidelines, Explanatory Memorandum* ¶ 62 (referring to accountability supported by legal sanctions); *EU Directive* art. 24 (unspecified sanctions for violations of directive); *see also CSA Model Code* ¶ 4.10.3 (discussing regulatory bodies receiving complaints of violations of fair information practice).

64. *IITF Report* § III.C (redress should be appropriate to violation).

65. The Commission's Deception Policy Statement recognizes that children can be unfairly exploited due to their age and lack of experience. *See* Deception Policy Statement, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 179 n.30 (1984), *citing Ideal Toy*, 64 F.T.C. 297, 310 (1964). For example, the Commission's actions regarding the marketing of pay-per-call 900 number services to children recognize children as a vulnerable group in the marketplace. *See Audio Communications, Inc.*, 114 F.T.C. 414 (1991) (consent order); *Teleline, Inc.*, 114 F.T.C. 399 (1991) (consent order); *Phone Programs, Inc.*, 115 F.T.C. 977 (1992) (consent order); *Fone Telecommunications, Inc.*, Docket No. C-3432 (June 14, 1993) (consent order). The Telephone Disclosure and Dispute Resolution Act of 1992 prohibits advertising of such services to children under the age of 12, unless the service is a bona fide educational service. 15 U.S.C. §§ 5701 *et seq*.

66. The Federal Educational Rights and Privacy Act of 1974 (FERPA), gives parents of minor students the right to inspect, correct, amend, and control the disclosure of information in education records. 20 U.S.C. § 1232g (1988). The Department of Health and Human Services Policy for Protection of Human Research requires parental/guardian written consent for all DHHS-funded research that involves children as subjects. 45 C.F.R. §§ 46.401-46.409 (1995). The Telephone Disclosure and Dispute Resolution Act of 1992 expressly prohibits advertising of pay-per-call (*e.g*., 900) services, except bona fide educational services, to children under 12. 15 U.S.C. §§ 5701 *et seq*. (Supp. IV 1992). The Children's Television Act of 1990, among other things, requires television stations and cable operators to limit the amount of advertising during children's television programming. 47 U.S.C. § 303a(b) (Supp. V 1994).

67. *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 [hereinafter "staff opinion letter"]. Commissioner Azcuenaga did not endorse all of the analyses and conclusions in the staff opinion letter.

68. Providing notice to parents raises some implementation issues, but where the child and parent have separate e-mail addresses, notice could be provided to the parent by e-mail.

69. Mechanisms for obtaining actual or verifiable parental consent include having the parent: mail or fax a signed form downloaded from the site; provide a credit card number; or provide an electronic (digital) signature. An e-mail message submitted without a digital signature may not be adequate to assure parental consent, since a site operator has no means of knowing whether the message is from a parent or a child. This is particularly true because most children do not currently have their own e-mail addresses and instead share their parents' e-mail addresses. While electronic signatures may be the best solution in the future, they may not be widely available at this point. In the meantime, children's Web sites may need to adopt traditional consent mechanisms, such as written consent forms and credit card numbers.

70. It is safe to assume that simply posting a privacy policy at a Web site or advising the child to seek parental permission before providing information online will have little impact on children. Many children will simply ignore these statements. Many will lack the sophistication or judgment to understand a privacy notice or to refrain from providing the requested information. Many children will be unwilling to wait for parental consent, and will provide whatever information is necessary to participate in the site's activity.

71. *See supra* Section III.A.1.

72. 63 Fed. Reg. 10,916 (1998).

73. The following trade associations and industry groups filed guidelines and/or principles: The Bankers Roundtable, Banking Industry Technology Secretariat ("BITS"); Direct Marketing Association ("DMA"); Electronic Messaging Association ("EMA"); Independent Bankers Association of America ("IBAA"); Individual Reference Services Group ("IRSG"); Interactive Services Association ("ISA"); Magazine Publishers of America ("MPA"); National Association of Federal Credit Unions ("NAFCU"); and Smart Card Forum ("SCF"). The Council of Better Business Bureaus, Inc.'s Children's Advertising Review Unit ("CARU") and the DMA also submitted guidelines addressing marketing to children, which are discussed in Section IV.B *infra*.

Numerous individual companies also filed their own privacy policies. Several other organizations and individuals also filed comments in response to the notice. Those filings, which are available for review on the Commission's Web site at http://www.ftc.gov, are not analyzed herein. The Commission's purpose in soliciting *trade association* and *industry group* guidelines was to assess industry's progress towards achieving a self-regulatory regime with respect to information collection online. While the Commission encourages individual companies to adopt information practice policies for the online environment, appreciates all of the submissions it has received in response to the Notice, and commends those firms that have developed effective self-regulatory policies, such policies, as well as the comments of other interested parties, do not constitute the elements of a self-regulatory system, which was the focus of the *Federal Register* Notice.

74. *See, e.g.*, NAFCU cover letter ("NAFCU does recommend that its members post privacy policies on their Web sites").

75. *See* ISA, *Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators*; DMA, *Marketing Online: Privacy Principles and Guidance*. The DMA encourages members to provide notice of, and substantive choice with respect to, internal secondary uses of information as well (*i.e.*, marketing back by the information collector).

76. The NAFCU submission is the only one that does not address choice.

77. *See* DMA, *Marketing Online: Privacy Principles and Guidance*; MPA submission.

78. *See* ISA, *Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators*.

79. *See* BITS and IBAA, *Privacy Principles* (BITS and IBAA each submitted the banking industry's *Privacy Principles* independently); SCF, *Consumer Privacy and Smart Cards—A Challenge and an Opportunity*; IRSG, *Individual Reference Services Industry Principles*.

80. *See generally* BITS and IBAA, *Privacy Principles*; NAFCU, *Recommended Privacy Policy*; SCF, *Consumer Privacy and Smart Cards—A Challenge and an Opportunity*; IRSG, *Individual Reference Services Industry Principles*.

81. *See* IRSG, *Individual Reference Services Industry Principles*; DMA, *The Committee on Ethical Business Practice Procedures for Case Handling*.

82. *See* IRSG, *Individual Reference Services Industry Principles*. The IRSG *Principles*, which constitute one model for self-regulation, require independent annual third-party audits, the results of which are made public, and limit the sharing of information with entities that do not adhere to the *Principles*. The DMA has also announced that, effective July 1999, adherence to certain fair information practices (notice and opt-out) will be mandatory for all members. *See* DMA Ethics and Consumer Affairs Department, *Case Report from the Direct Marketing Association's Committee on Ethical Business Practice* (Sept.-Nov. 1997) at 4.

83. The DMA Committee on Ethical Business Practice investigates complaints against companies alleged to be violating DMA's voluntary guidelines. In cases in which a satisfactory resolution of a complaint is not reached, the name of the company and the facts of the case are made public. In addition, the Committee may refer cases to law enforcement agencies and/or to the DMA's Board of Directors for further action including censure, suspension and/or expulsion of a member. This peer review process is non-binding. DMA, *The Committee on Ethical Business Practice Procedures for Case Handling*.

84. Both BITS and IBAA submitted BITS's *Privacy Principles Implementation Plan*. The BITS plan states that establishment of a privacy mark may be necessary, calls upon banks to "apply their own internal process to assure compliance with the bank's privacy principles," and states that "[b]reaches of policy will be addressed internally on a case-by-case basis by each bank." This non-binding reference to ensuring compliance with policies is the only reference to enforcement in any of the submitted guidelines, other than the IRSG *Principles* and the DMA Committee on Ethical Business Practice discussed above.

85. CARU was established by the advertising community as an independent manager of the industry's self-regulatory programs in 1974. Its main activity is the review and evaluation of child-directed advertising in all media. Its Board of Directors consists of representatives from the Council of Better Business Bureaus, the American Association of Advertising Agencies, the American Advertising Federation, and the Association of National Advertisers. CARU is funded directly by members of the children's advertising industry. The DMA represents more than 3,600 member companies interested in database marketing. Its members include catalogers, financial services, publishers, book and music clubs, retail stores, industrial manufacturers, and service industries. Copies of both CARU's and DMA's guidelines are found in Appendix E.

86. The *CARU Guidelines* address children under age 12, while the *DMA Children's Guidelines* do not provide a definition for the term "children."

87. *CARU Guidelines* at 1, 3. The *CARU Guidelines* do not define "passive tracking." However, the term refers to information collected by using navigational software designed to reveal information about the visitor's experience on the site, such as the pages visited, the information downloaded, the content viewed, the operating system used, and the referring site's Internet address.

88. *Id.* at 4.

89. *Id.*

90. *Id.*

91. *Id.*

92. CARU is one of the few trade groups that implements a voluntary enforcement mechanism for both its online privacy guidelines as well as its general media guidelines. In addition to its own monitoring of advertisers, CARU initiates investigations upon receipt of a complaint from a consumer or a company. CARU then seeks the advertiser's compliance with its guidelines and publishes its case reports. If a company is uncooperative and the practices are allegedly deceptive or unfair, CARU refers the matter to the Commission. CARU's voluntary enforcement

mechanism is modeled on that of the National Advertising Division (NAD), which is also associated with the Council of Better Business Bureaus, Inc.

93. Since CARU's founding in 1974, 98% of the subjects of its investigations have complied with its decisions.

94. The *CARU Guidelines* apply generally to marketers of children's products and services. Since CARU is not a membership organization, however, adherence to its guidelines is not mandatory. Each of CARU's leading organizational sponsors has urged its own members to implement the *CARU Guidelines*, but these sponsors do not make adherence mandatory for their members.

95. The *DMA Children's Guideline*s suggest that marketers use language such as "Your mom or dad should say it's okay for you to answer these questions," but are not explicit with respect to when parental permission should be sought. *DMA Children's Guidelines*, Guideline No. 1.

96. *DMA Children's Guidelines*, Guideline Nos. 1-2.

97. McCain/Bliley letters. Specifically, the Commission stated that "[w]e hope to find by March 1, 1998, that a substantial majority of commercial Web sites are clearly posting their information practices and privacy policies." *Id*. at n.2.

98. The samples for groups A-D were drawn from a comprehensive list of commercial Web sites provided by the Dun and Bradstreet Corporation. *See* Appendix A.

99. The terms "likely to be of interest to consumers" and "primarily directed to children aged fifteen or younger" are defined in Appendix A.

100. For a copy of the Survey Forms used by the surfers, see Appendix C.

101. These figures are based on data supplied by The Dun & Bradstreet Corporation. Figures do not total 100%. Approximately 3% of the sites in all the samples are not classified by size, because sales figures were unavailable. For a description of the Dun & Bradstreet database used in this survey, see Appendix A.

102. *See* Appendix D, Table 1.

103. *See* Appendix D, Table 1.

104. *See* Appendix D, Table 1.

105. Company size information was not obtained for Web sites in this sample.

106. *See supra* Section II.B.

107. The rates are: 92% of the sites in the Comprehensive Sample; 88% of the Health Sample sites; 87% of the Retail Sample sites; 97% of the Financial Sample sites; and 97% of the Most Popular Sample sites. *See* Appendix D, Table 3, which also sets forth statistics based upon company size.

108. For purposes of this survey, the provision of a mechanism for sending e-mail to a site's Webmaster, without more, was not considered collection of an e-mail address. A site's invitation to online consumers to "Contact Us" or "Send Us Your Comments" by e-mail, however, was deemed to be collection of an e-mail address. When the collection of an e-mail address is not considered, the number of sites collecting personal information decreases slightly in all samples. Thus, 65% of all sites in the Comprehensive Sample collect some personal information other than an e-mail address; as do 53% of the sites in the Health Sample; 67% of the sites in the Retail Sample; 73% of the sites in the Financial Sample; and 94% of the sites in the Most Popular Sample. *See also infra* note 115. Because the survey form did not identify the manner of e-mail collection, the above statistics exclude *all* sites that collect only an e-mail address, including those sites that ask for it in contexts other than "Contact Us," such as on registration forms, etc.

109. For similar information with respect to the other samples, see Appendix D, Table 5.

110. *See* Appendix D, Table 4.

111. *Id*.

112. The Commission cannot report on the number of companies in the survey that create such profiles, because the survey concerns Web sites' disclosures, and not actual practices.

113. The numbers for the Health, Retail and Financial samples are as follows: sites collecting five or more additional types of information — 12% (Health), 19% (Retail), 26% (Financial); sites collecting three or more additional types of information — 36% (Health), 60% (Retail), 53% (Financial); sites collecting at least one additional type of information — 57% (Health), 76% (Retail), 73% (Financial). *See* Appendix D, Table 6.

114. *See* Appendix D, Table 2.

115. *See* Appendix D, Table 7. The percentage of disclosures among sites that collect some personal information other than an e-mail address is slightly higher: 21% in the Comprehensive Sample; 24% in the Health Sample; 18% in the Retail Sample; 22% in the Financial Sample; and 74% in the Most Popular Sample. *See also supra* note 108.

116. *See* Appendix D, Table 8.

117. *See* Appendix D, Table 9.

118. *See* Appendix D, Table 2.

119. *See* Appendix D, Table 7.

120. *See* Appendix D, Table 8.

121. *See* Appendix D, Table 9. Some sites post both a Privacy Policy Notice and one or more Information Practice Statements.

122. *See, e.g.*, Communications Daily (Untitled, February 10, 1998); Washington Telecom Newswire (Untitled, February 9, 1998); I. Teinowitz, "*FTC Will Survey Marketer Web Sites for Privacy*," Advertising Age (February 1998), available at http://www.adage.com/interactive/articles/19980216/article1.html.

123. *See* Appendix D, Table 7.

124. Given the small number of sites involved, statistics based upon company size have not been reported.

125. The rate is 33% (or 31 sites) for the Comprehensive Sample, 32% (or 6 sites) for the Health Sample, 33% (or 6 sites) for the Retail Sample, and 35% (or 7 sites) for the Financial Sample. *See* Appendix D, Table 10. In responding to the relevant question on the General Survey Form, staff counted both statements giving choice regarding internal uses of the personal information and statements giving choice about the transfer of the information to third parties as statements offering consumers choice about how the information collected will be used. *See* Appendix C.

126. The rate is 10% (or 9 sites) for the Comprehensive Sample. *See* Appendix D, Table 10.

127. The rate is 6% (or 1 site) for the Retail Sample and 5% (or 1 site) for the Financial Sample. *See* Appendix D, Table 10.

128. *See* Appendix D, Table 11. The rate for the Health Sample is 32% (or 6 sites) and the rate for the Retail Sample is 22% (or 4 sites). Statements such as "We keep this information confidential" were counted as assertions of non-disclosure to third parties.

129. *See* Appendix D, Table 11. Statements indicating that demographic or interest information may be shared with third parties were counted as assertions of possible third-party disclosures.

130. *See* Appendix D, Table 12. When expressed as a percentage of *all* sites in a given sample (and not just those sites that collect personal information and have an information practice disclosure), the percent of sites offering choice, access, or security, or addressing disclosures to third parties, is even lower. Thus, only 5% of all sites in the Comprehensive Sample, 4% of all sites in the Health and Retail Samples, and 6% of all sites in the Financial Sample state that they

offer consumers choice; 1% of all sites in the Comprehensive Sample, 2% of all sites in the Retail Sample and no sites in the Health and Financial Samples state that they offer consumers access; 2% of all sites in the Comprehensive Sample, no sites in the Health Sample, and 1% of all sites in the Retail and Financial Samples state that they take data security measures; 5% of all sites in the Comprehensive Sample, 4% of all sites in the Health Sample, and 3% of all sites in the Retail and Financial Samples state that they will not disclose any personal information collected to third parties; and 5% of all sites in the Comprehensive Sample, 4% of all sites in the Health and Retail Samples, and 6% of all sites in the Financial Sample state that they may disclose some or all of the personal information collected to third parties.

131. *See* Appendix D, Table 10.

132. *Id.*

133. *Id.*

134. *See* Appendix D, Table 11.

135. *Id.* Again, the above figures are significantly lower when expressed as a percentage of *all* sites in the Most Popular Sample. Thus, 49% of all sites in the Most Popular Sample state that they offer consumers choice; 27% state that they offer consumers access; 12% state that they take data security measures; 10% state that none of the personal information collected will be disclosed to third parties; and 56% state that some or all of the personal information collected may be disclosed to third parties.

136. *See* Appendix D, Table 12.

137. *See* Appendix D, Table 3.

138. *See* Appendix D, Table 13.

139. As in the General Survey, a mere hyperlink to a site's Webmaster was not considered collection of an e-mail address for purposes of this survey. However, hypertext that asks visitors to "Contact Us" or "Send Us Your Comments" was included as collection of an e-mail address. *See supra* note 108.

140. *See* Appendix D, Table 5.

141. *See* Appendix D, Table 6.

142. For instance, in order to register for certain online activities, some sites require children to identify their interests such as rollerblading, skateboarding, ice skating, biking, video games, science, football, soccer, and computer games. Other sites ask children information about their

favorite television shows, commercials, and musical groups.

143. For example, one site asks children personal financial questions such as the following:

> Do you own mutual funds?
> Are your parents currently saving for your college education?
> What do you usually do with gifts of money?

144. *See* Appendix D, Table 2. The higher disclosure rate for the Children's Sample may reflect the fact that staff publicly disclosed that this sample would be selected from sites listed in the Yahooligans! Directory.

145. *Id.*

146. *See* Appendix D, Table 9.

147. *See* Appendix D, Table 8.

148. *See* Appendix D, Table 10.

149. *Id.*

150. *Id.*

151. *Westin Survey* at 3.

152. *See* Appendix D, Table 13.

153. *See* Appendix D, Table 11.

154. *Id.*

155. *See* Appendix D, Table 13.

156. *Id.*

157. *Id.*

158. *Id.* Examples of opt-out statements include: "When minors subscribe to the newsletter, they are asked for their parent's e-mail informing them [sic] their kid has subscribed to the e-mail and the parent has the option to discontinue this subscription," and "All parents can correct or remove any information we receive from a child by contacting us online, by phone or mail."

159. *Westin Survey* at 3.

160. Current American privacy law can best be described as sectoral, consisting of a handful of disparate statutes directed at specific industries that collect personal data and none of which specifically covers the collection of personal information online. *See, e.g.*, Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 *et seq*. (governing consumer credit reports); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 *et seq*. (governing electronic mail and voicemail communications); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (governing cable television subscriber information); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 *et seq*. (governing individual bank records); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (governing video rental records); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (governing student records); Communications Act of 1934, *as amended by*, Telecommunications Act of 1996, 47 U.S.C. § 222 (governing information relating to use of telecommunication services ["customer proprietary network information"]); *cf.* Privacy Act of 1974, 5 U.S.C. § 552a (governing data collected by the federal government). Pursuant to the Supreme Court's decision in *United States v. Miller*, 425 U.S. 435 (1976), individuals have no Fourth Amendment interest in personal information they voluntarily have conveyed to another. Consequently, any privacy protections for personal information must be legislatively grounded.

161. 15 U.S.C. §§ 41 *et seq*.

162. *See supra* note 67.

163. Parental notice raises some implementation issues. In those instances where parents and children have separate e-mail addresses, notice may be provided to parents electronically. Where verifiable parental consent is required, sites can simply direct children to download (print) the notice and consent form and have the parent return the signed form by regular mail or facsimile.

APPENDIX A: METHODOLOGY

APPENDIX B: SURFER INSTRUCTIONS (GENERAL AND CHILDREN'S SURVEYS)

APPENDIX C: SURVEY SAMPLES AND RESULTS

APPENDIX D: SUPPORTING DATA TABLES

APPENDIX E: INDUSTRY GUIDELINES