

---

## **Clinton Presidential Records Digital Records Marker**

---

This is not a presidential record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

This marker identifies the place of a publication.

---

Publications have not been scanned in their entirety for the purpose of digitization. To see the full publication please search online or visit the Clinton Presidential Library's Research Room.

---

# Site-Seeing

ON THE INTERNET



A publication from the Federal Trade Commission and the National Association of Attorneys General



# PRIVACY ONLINE: A REPORT TO CONGRESS

*JS Nany*

## A SUMMARY OF SURVEY METHODOLOGY<sup>1</sup>

The Commission surveyed over 1,400 Web sites in March 1998. The survey drew random samples of Web sites from six different groups:

- ◆ all commercial U.S. sites “likely to be of interest to consumers” (group A);
- ◆ all consumer-oriented U.S. sites in the health, retail, and financial sectors (groups B, C, and D, respectively);
- ◆ all U.S. commercial sites “primarily directed to children aged fifteen or younger” (group E); and
- ◆ the most popular U.S. commercial sites (group F).

The Dun & Bradstreet Corporation’s (“D&B”) Electronic Commerce Registry database served as the starting point for creating the pools from which groups A through D were drawn. The database matches names and addresses registered by InterNIC, the official domain name registry, with D&B’s database of 49 million businesses worldwide and provides a comprehensive listing of commercial Web sites. The sites for group A were chosen from all “.com” sites appearing in the D&B database, with the exception of insurance-related sites. Commission staff chose sites from the database for the Health, Retail, and Financial sector samples based upon classifications that identify businesses according to their primary source of revenue. The children’s sites were drawn from Web sites in the “Yahooligans!” Directory, an online directory for children compiled by “Yahoo!”. The most popular sites on the Web were selected from three sources: (i) Media Metrix, The PC Meter Company; (ii) RelevantKnowledge; and (iii) Web21’s “100-Hot.com.” The three sources’ separate lists of the one hundred most popular sites were combined and the Most Popular Sample consists of the 111 qualifying sites that appeared on at least one of the three source lists.

A systematic sampling procedure was then used to select sites in each group described above. These sites were then randomly examined by forty Commission staff members (“surfers”). Each surfer underwent a full day’s training in the technical skills of visiting and reviewing Web sites and in use of the survey forms. Surfers were randomly assigned Internet addresses from each group. Once a site was accessed, surfers were first required to determine whether the site qualified for inclusion in the sample—*i.e.*, whether the site was “likely to be of interest to consumers,” or, in the case of the children’s sample, whether the site was “primarily directed” to children aged 15 or under. The final sample sizes of qualifying sites are: 674 sites in the Comprehensive Sample of commercial Web sites generally (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).

Once a surfer concluded that a site qualified for inclusion in one of the samples, 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 to determine whether it discloses its information practices. In the case of the Children's Sample, a supplemental survey form was used to review sites after the primary survey was completed to analyze whether and how those sites addressed notice and choice for parents. The Children's Sample also tracked information collected *from children*. In this regard, information collected in connection with a payment form (requiring a credit card number, check, or money order) was deemed to be collected from adults; all other information collection at children's sites was considered information collected from children.

Numerous measures were taken to ensure the quality and accuracy of the data collected by the surfers. Each site was surveyed by a second surfer who revisited the site to ensure the accuracy of the information reported on the survey form for that site. The completed survey forms for sites found to be posting an information practice disclosure, along with the print-outs of those disclosures, were then reviewed for errors a third time by a group of four proctors. Once the survey forms for all samples had undergone these multiple levels of review, the same data were entered into two separate databases by separate data entry personnel and the two databases were electronically compared. The data analysis itself was also conducted twice, by separate individuals utilizing different analytic tools. The results of these analyses—the statistics reported in the report—were then compared to ensure uniformity and accuracy.

<sup>1</sup> A more complete description of the Survey's methodology can be found in Appendix A.

---



# **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 .....                                                                             | i  |
| I. Introduction .....                                                                               | 1  |
| II. History and Overview .....                                                                      | 2  |
| A. The Federal Trade Commission's Approach to Online Privacy .....                                  | 2  |
| B. Consumer Privacy Online .....                                                                    | 2  |
| 1. Growth of the Online Market .....                                                                | 2  |
| 2. Privacy Concerns .....                                                                           | 3  |
| C. Children's Privacy Online .....                                                                  | 4  |
| 1. Growth in the Number of Children Online .....                                                    | 4  |
| 2. Safety and Privacy Concerns .....                                                                | 4  |
| III. Fair Information Practice Principles .....                                                     | 7  |
| A. Fair Information Practice Principles Generally .....                                             | 7  |
| 1. Notice/Awareness .....                                                                           | 7  |
| 2. Choice/Consent .....                                                                             | 8  |
| 3. Access/Participation .....                                                                       | 9  |
| 4. Integrity/Security .....                                                                         | 10 |
| 5. Enforcement/Redress .....                                                                        | 10 |
| B. Application of Fair Information Practice Principles to Information Collected From Children ..... | 12 |
| 1. Parental Notice/Awareness and Parental Choice/Consent .....                                      | 12 |
| 2. Access/Participation and Integrity/Security .....                                                | 13 |
| IV. Industry Association Guidelines .....                                                           | 15 |
| A. Industry Association Guidelines .....                                                            | 15 |
| 1. Notice/Awareness .....                                                                           | 15 |
| 2. Choice/Consent .....                                                                             | 16 |
| 3. Access/Participation .....                                                                       | 16 |
| 4. Integrity/Security .....                                                                         | 16 |
| 5. Enforcement/Redress .....                                                                        | 16 |
| B. Guidelines Regarding Children's Information .....                                                | 17 |
| V. Survey of Commercial Web Sites .....                                                             | 19 |
| A. Overview .....                                                                                   | 19 |
| B. General Survey Findings .....                                                                    | 21 |
| 1. Web Sites .....                                                                                  | 21 |
| 2. Personal Information Collection .....                                                            | 22 |
| 3. Frequency of Disclosures .....                                                                   | 27 |
| 4. Nature of Disclosures .....                                                                      | 29 |
| C. Children's Survey Findings .....                                                                 | 31 |

|                                                                  |    |
|------------------------------------------------------------------|----|
| 1. Personal Information Collection from Children .....           | 31 |
| 2. Frequency of Disclosures .....                                | 34 |
| 3. Nature of Disclosures .....                                   | 35 |
| 4. Parental Involvement .....                                    | 37 |
| VI. Conclusions .....                                            | 39 |
| Endnotes .....                                                   | 45 |
| 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                                  |    |

## **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").<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup>

### **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.”<sup>4</sup>

The online consumer market is growing exponentially. In early 1997, 51 million adults were already online in the U.S. and Canada,<sup>5</sup> and 73% reported that they had shopped for product information on the World Wide Web.<sup>6</sup> 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.<sup>7</sup> Analysts estimate that Internet advertising — which totaled approximately \$301 million in 1996 — will swell to \$4.35 billion by the year 2000.<sup>8</sup>

## **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.<sup>9</sup> 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.<sup>10</sup> 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.<sup>11</sup> Clearly, consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections.<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup> Their growing presence online, therefore, creates enormous opportunities for marketers to promote their products and services to an eager audience.<sup>18</sup> 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.<sup>19</sup> 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.<sup>20</sup> 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.<sup>21</sup> 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.<sup>22</sup>

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.<sup>23</sup> Children generally lack the developmental capacity and judgment to give meaningful consent to the release of personal information to a third party.<sup>24</sup> 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.<sup>25</sup>

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.<sup>26</sup>

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.<sup>27</sup> The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.<sup>28</sup> 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.<sup>29</sup> 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.<sup>30</sup>

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;<sup>31</sup>
- identification of the uses to which the data will be put;<sup>32</sup>
- identification of any potential recipients of the data;<sup>33</sup>

- 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);<sup>34</sup>
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information;<sup>35</sup> and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.<sup>36</sup>

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

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.<sup>42</sup> 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.<sup>43</sup> 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.<sup>44</sup> 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.<sup>45</sup>

### **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.<sup>46</sup> 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.<sup>47</sup>

#### **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.<sup>48</sup>

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.<sup>49</sup> 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.<sup>50</sup>

#### **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.<sup>51</sup> 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.<sup>52</sup>

##### **a. Self-Regulation<sup>53</sup>**

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).<sup>54</sup> 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;<sup>55</sup> external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.<sup>56</sup> A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.<sup>57</sup>

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.<sup>58</sup> 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.<sup>59</sup>

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.<sup>60</sup> 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.<sup>61</sup> 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;<sup>62</sup> 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.<sup>63</sup> Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.<sup>64</sup>

## **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.<sup>65</sup> 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.<sup>66</sup>

### **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.<sup>67</sup> 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,<sup>68</sup> 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*<sup>69</sup> to its collection.<sup>70</sup>

The content of the notice should include at a minimum, the elements described above,<sup>71</sup> 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.<sup>72</sup> Nine industry-specific guidelines were submitted.<sup>73</sup> 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,<sup>74</sup> 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.<sup>75</sup> 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.<sup>76</sup> 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);<sup>77</sup> others suggest giving consumers a choice solely with respect to external uses.<sup>78</sup> 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.<sup>79</sup> 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.<sup>80</sup>

## **5. ENFORCEMENT/REDRESS**

With limited exception,<sup>81</sup> the submitted guidelines contain no enforcement mechanisms. Only one of the guidelines conditions further membership and information sharing on adherence to the guidelines.<sup>82</sup> One other set of guidelines provides for peer review of alleged violations, but it is not binding.<sup>83</sup> All of the other guidelines and policies submitted are merely exhortatory.<sup>84</sup> 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").<sup>85</sup> Both guidelines address younger children.<sup>86</sup>

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."<sup>87</sup> In all cases, the notice must specify the means by which parents can correct or remove the information collected from a company's database.<sup>88</sup> 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.<sup>89</sup> 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.<sup>90</sup> If a site collects only anonymous or aggregate information, the guidelines require notice of the intended uses of the information, but not parental consent.<sup>91</sup>

In addition, CARU has an enforcement mechanism in place to promote compliance with its online privacy guidelines,<sup>92</sup> and has achieved a remarkably high level of compliance under this mechanism in the offline media over a long period of time.<sup>93</sup> 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.<sup>94</sup>

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;<sup>95</sup> and (3) support parental control over the collection of data from children through notice and opt-out.<sup>96</sup> 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.<sup>97</sup> 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;<sup>98</sup> 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.<sup>99</sup> 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.<sup>100</sup> 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).<sup>101</sup>

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).<sup>102</sup>

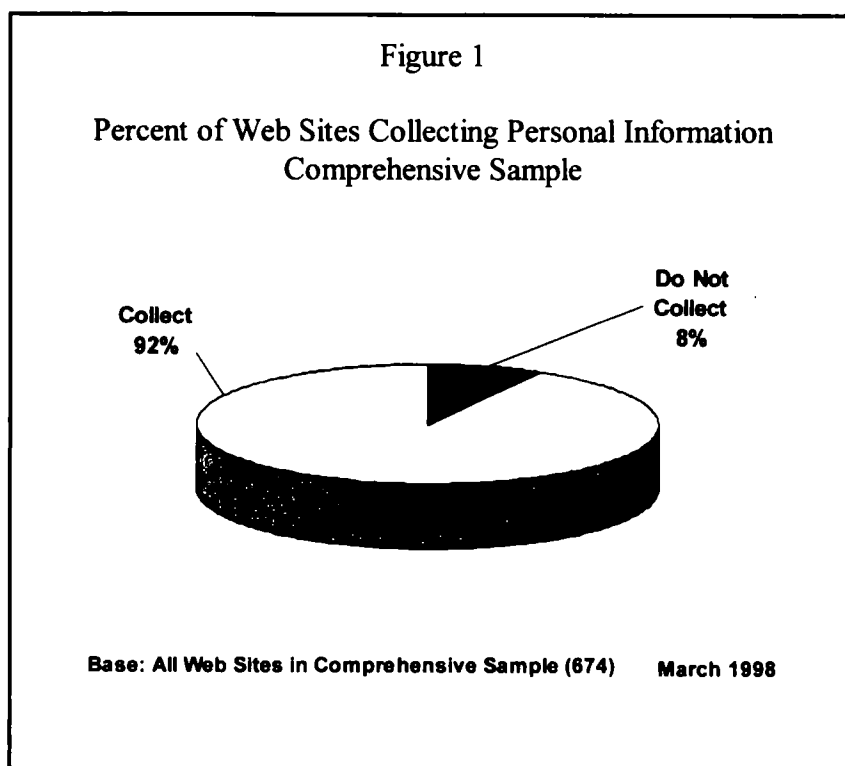
The Retail and Financial Samples (Samples C and D) are similarly diverse. The range of consumer goods and services sold by the companies represented in the Retail Sample (Sample C) mirrors the variety found in the Comprehensive Sample. Sellers of photographic equipment, automobiles, cigars, jewelry, 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.<sup>103</sup> 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.<sup>104</sup>

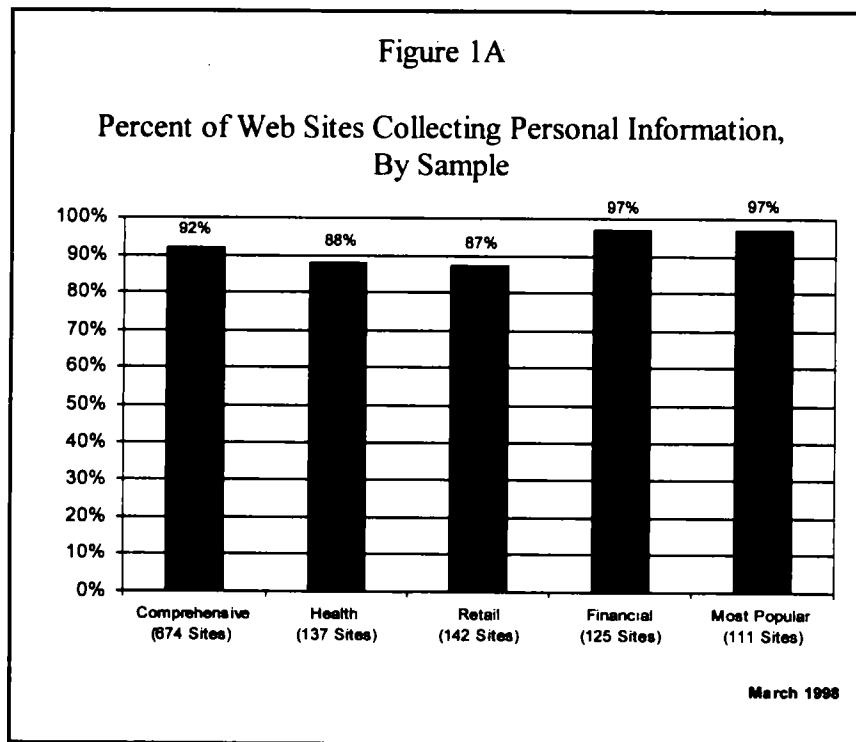
The Most Popular Sample (Sample F) includes 111 of the most popular sites on the Web. Companies represented in this sample include search engines, Internet service providers, electronic mail services, software and computer companies, news and information companies, online directories, entertainment companies,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

## **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.<sup>106</sup> 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.<sup>107</sup> 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.

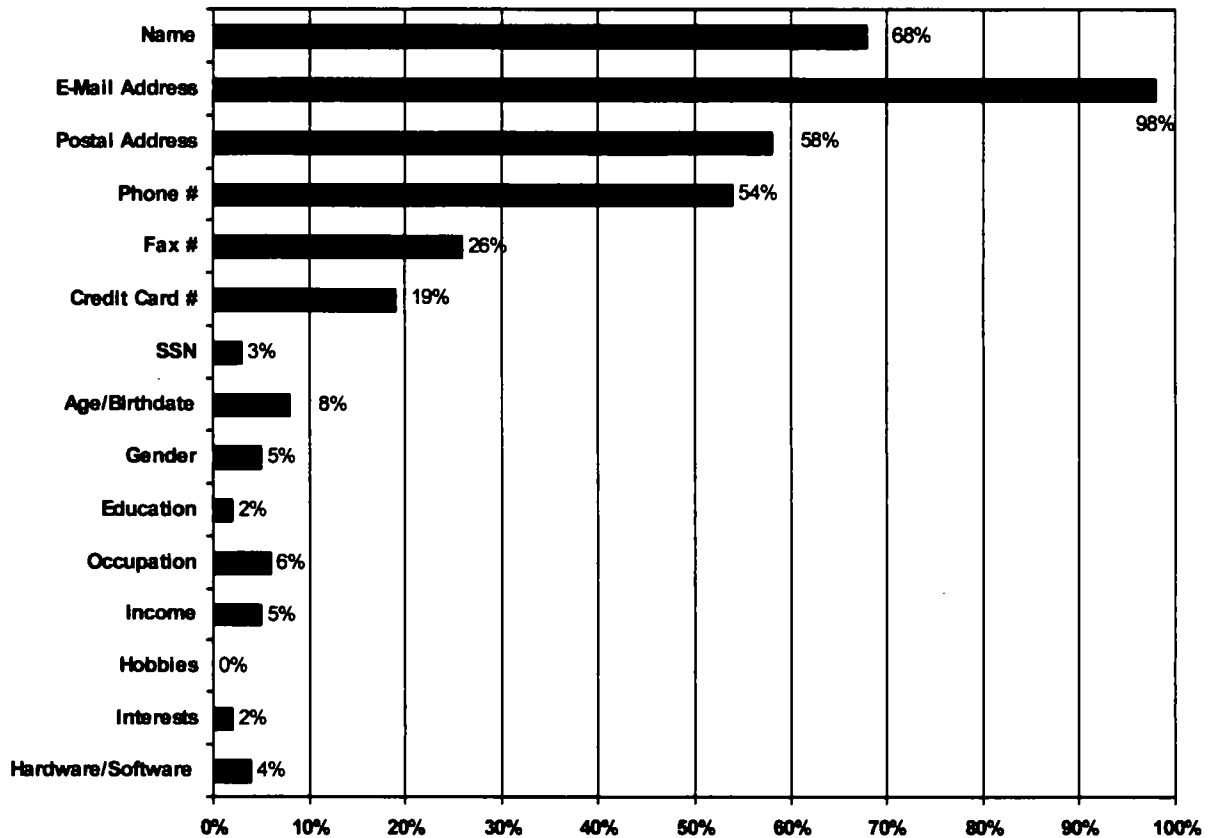




These Web sites collect a remarkable variety of personal information, including name, e-mail address,<sup>108</sup> postal address, telephone number, fax number, credit card number, Social Security number, age or date of birth, gender, education, occupation, income, hobbies, interests, and the type of 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.<sup>109</sup>

Figure 2

Types of Personal Information Collected  
Comprehensive Sample



Base: Web sites in Comprehensive Sample that collect personal information (621)

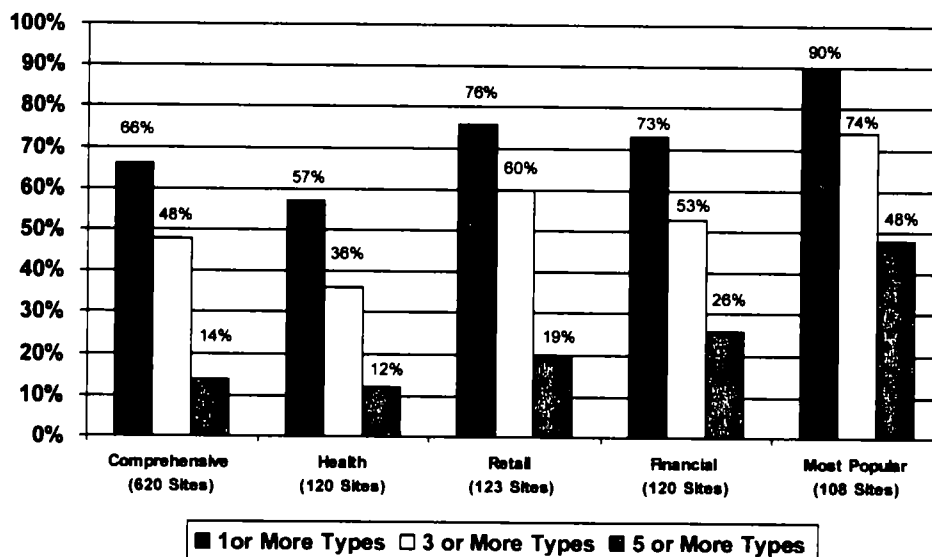
March 1998

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.<sup>110</sup> 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.<sup>111</sup> 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.<sup>112</sup>

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.<sup>113</sup>

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

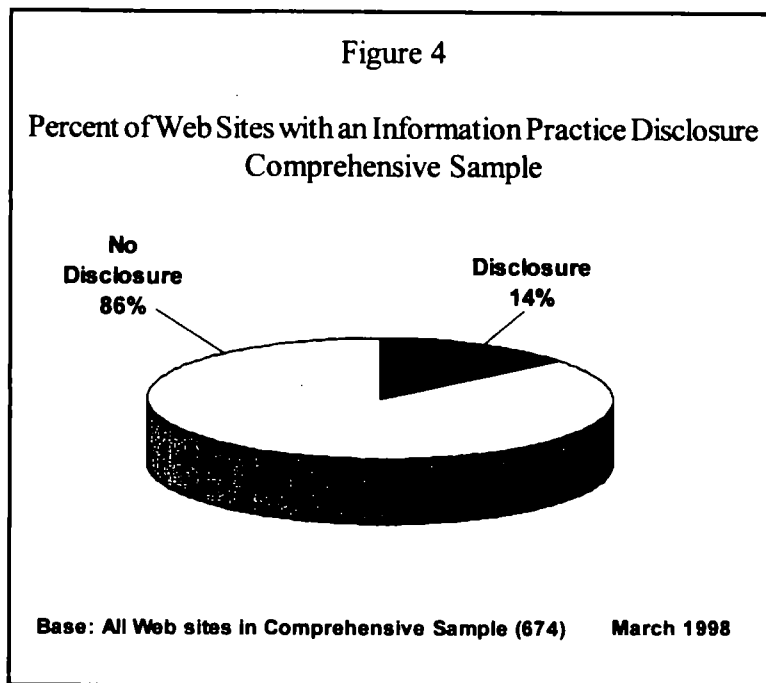


March 1998

### 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.<sup>114</sup>

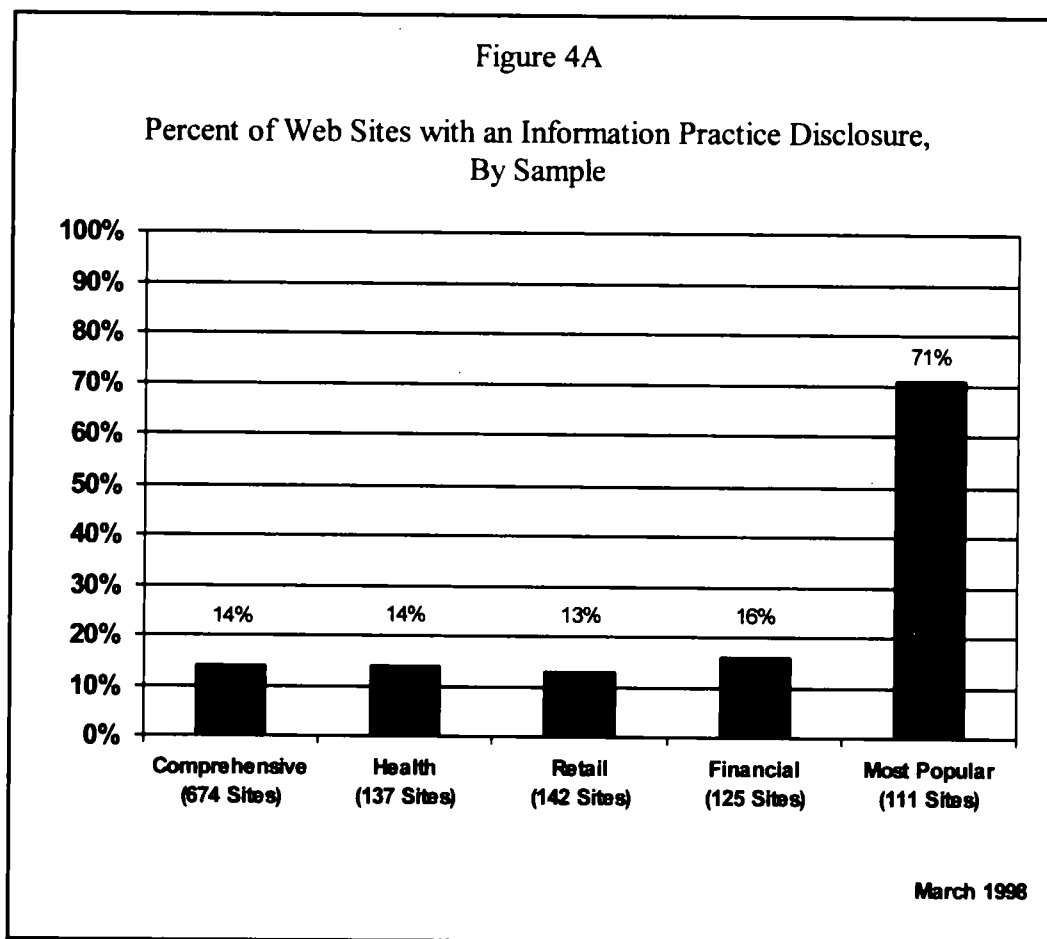


Among sites in the random samples that collect personal information, the disclosure rate is equally low. Of these sites, only 15% in the Comprehensive Sample, 16% in the Health Sample, 15% in the Retail Sample, and 17% in the Financial Sample have any information practice disclosure.<sup>115</sup> Only 2% of the sites that collect personal information in each of these samples have a Privacy Policy Notice.<sup>116</sup> 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.<sup>117</sup>

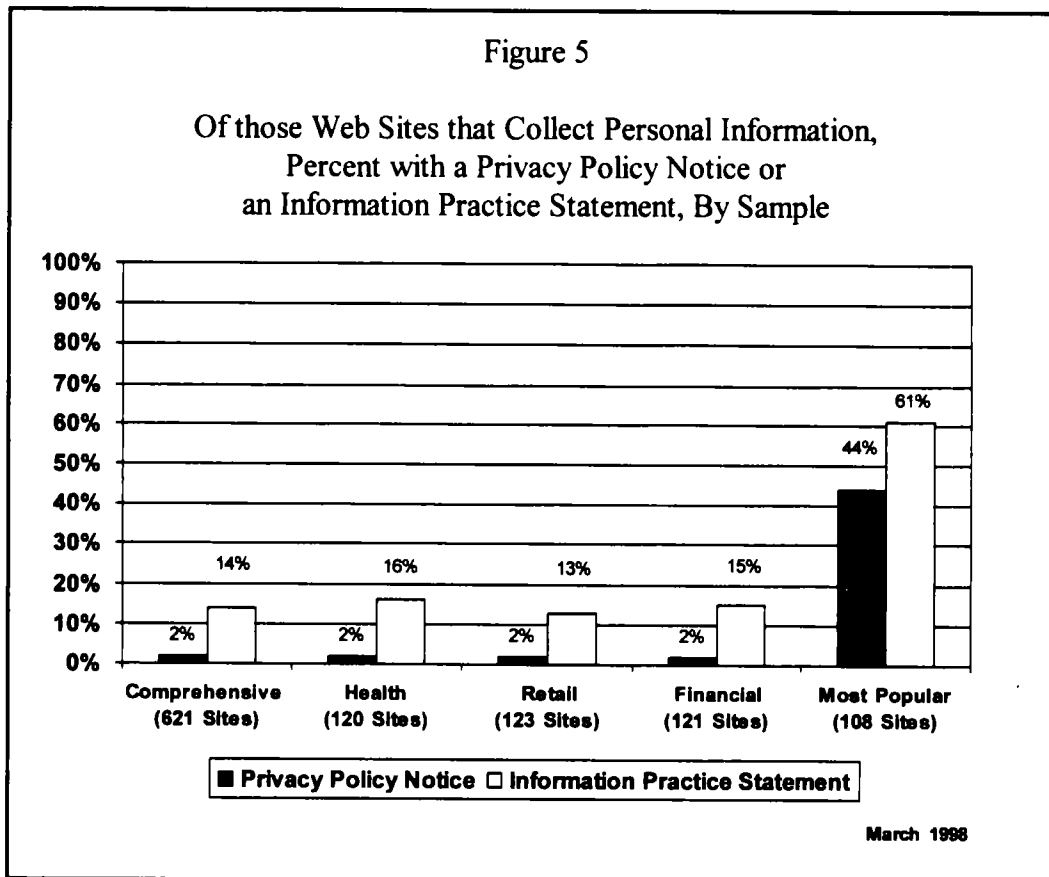
**b. Most Popular Sample**

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),<sup>118</sup> and 73% of sites that collect personal information have such a disclosure.<sup>119</sup> Of the sites in this sample that collect personal information,



44% have a Privacy Policy Notice,<sup>120</sup> and 61% have at least one Information Practice Statement.<sup>121</sup> 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.<sup>122</sup> However, despite this clear public notice, over one-quarter of these sites still failed to post an information practice disclosure.



#### 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.<sup>123</sup> 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.<sup>124</sup>

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.<sup>125</sup> 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.<sup>126</sup> 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.<sup>127</sup>

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.<sup>128</sup> 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.<sup>129</sup> 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.<sup>130</sup>

#### **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,<sup>131</sup> 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,<sup>132</sup> and 16% (or

13 sites) state that they take steps to provide security for the personal information collected after they receive it.<sup>133</sup>

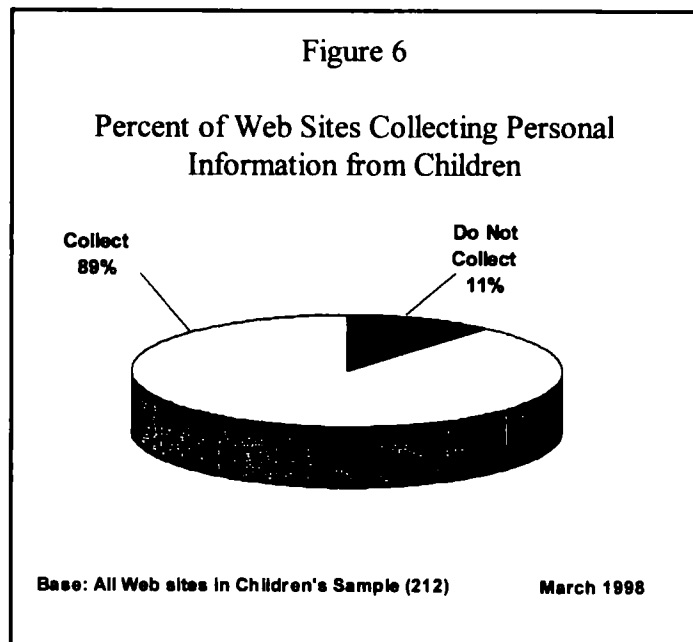
Fourteen percent (or 11 sites) of the sites in this sample that collect personal information and have an information practice disclosure say that none of the personal information they collect will be disclosed to third parties.<sup>134</sup> Seventy-eight percent (or 62 sites) of these sites state that at least some of the personal information collected may be released to third parties.<sup>135</sup> 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.<sup>136</sup>

## **C. CHILDREN'S SURVEY FINDINGS**

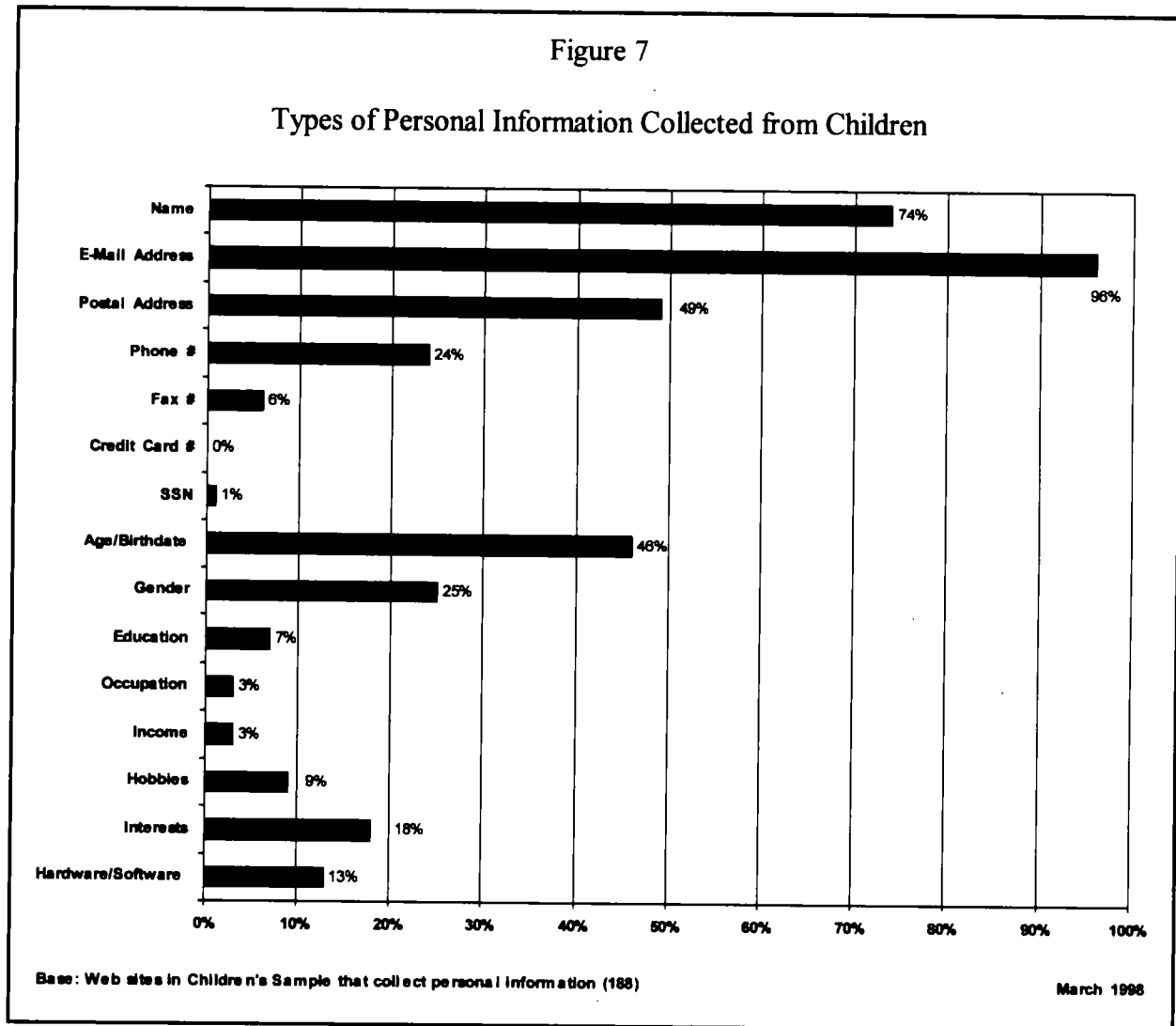
### **1. PERSONAL INFORMATION COLLECTION FROM CHILDREN**

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)<sup>137</sup> and that 88% collect at least one type of personal identifying information as well.<sup>138</sup> Personal information collected from children

includes a wide array of identifying information such as name, e-mail address,<sup>139</sup> postal address,



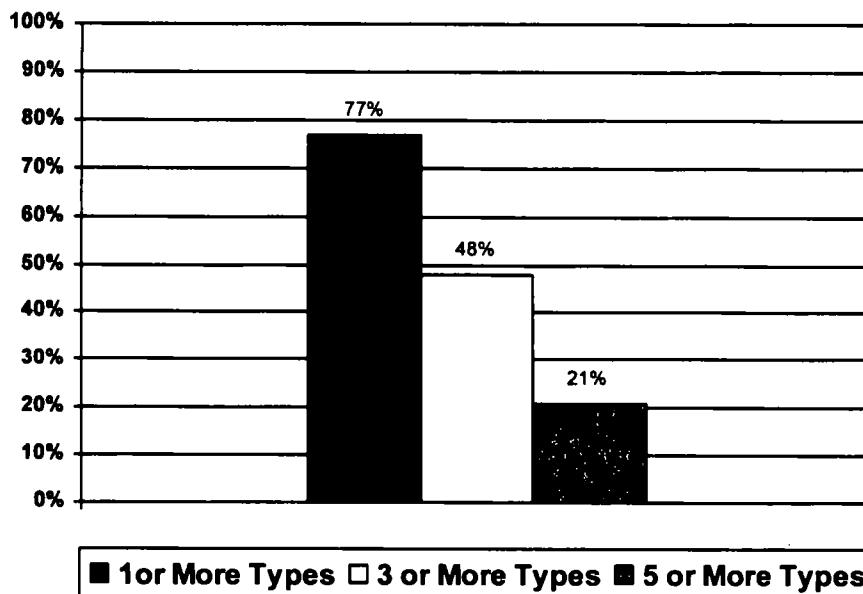
telephone number, and Social Security number, as well as other personal information like age or date of birth, gender, education, interests, and hobbies.<sup>140</sup>



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.<sup>141</sup>

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)

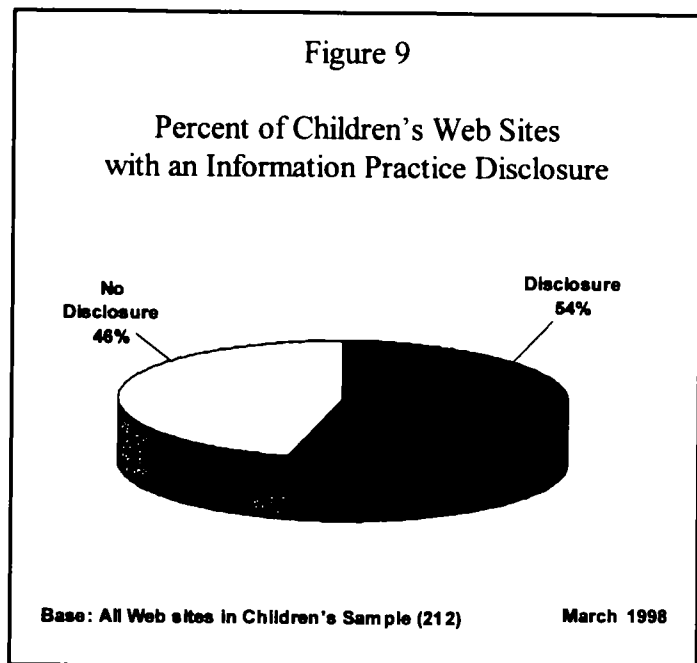
March 1998

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.<sup>142</sup> 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.<sup>143</sup>

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.<sup>144</sup> 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.<sup>145</sup>



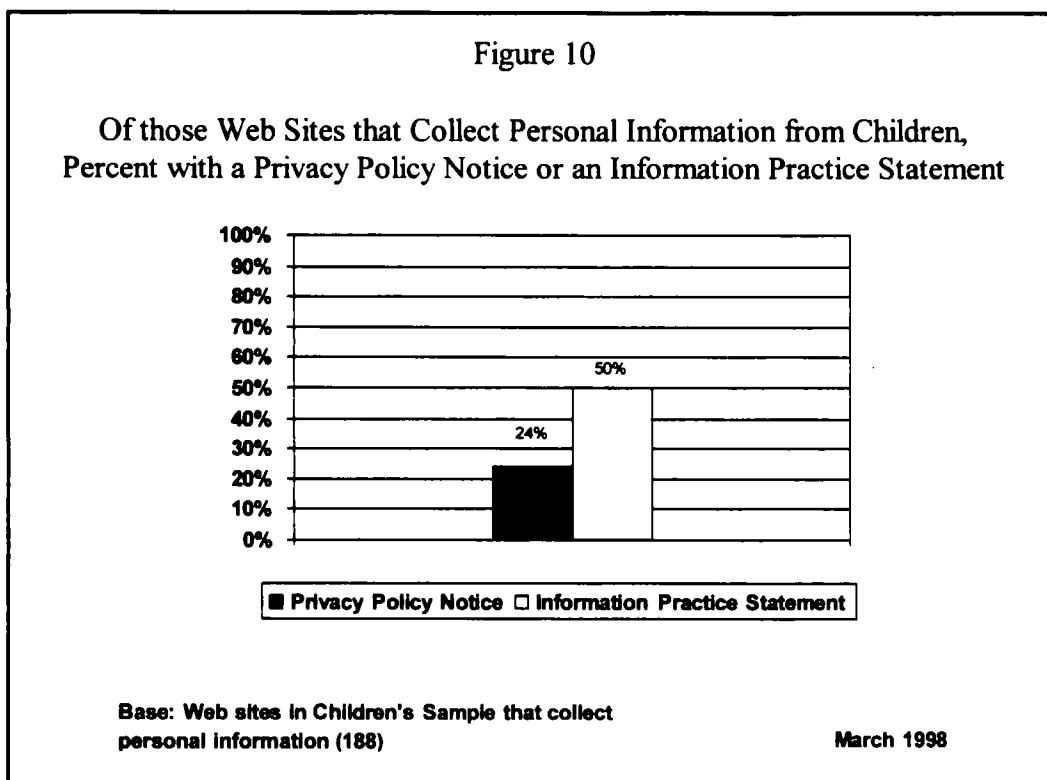
As noted above with respect to the general samples, staff applied a very broad definition of what constitutes an Information Practice Statement. Any statement that describes a particular use or practice regarding consumers' personal information and/or a choice offered to consumers about their personal 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

- 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.<sup>146</sup>

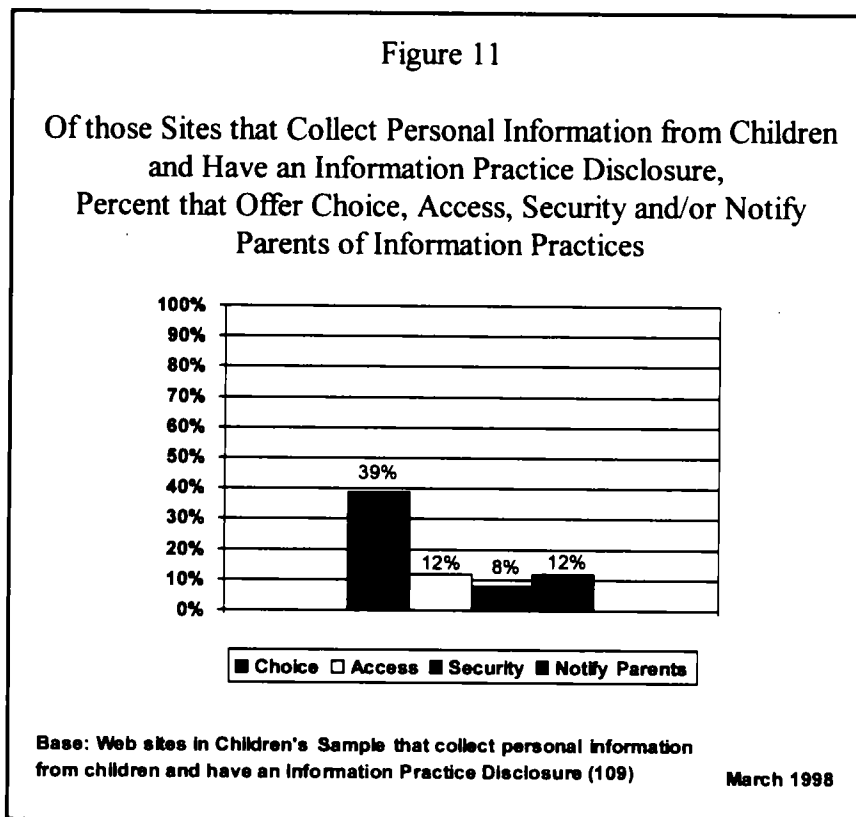
Although a majority of children's sites have some statement about one or more of their information practice(s), the number of children's sites that have a Privacy Policy Notice is much lower. Twenty-four percent of the sites that collect personal information from children post a Privacy Policy Notice.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



### 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.<sup>148</sup> Only 12% (or 13 sites) of these sites say that they offer access to this personal information or an opportunity to correct inaccuracies.<sup>149</sup> 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).<sup>150</sup> 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.



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.<sup>151</sup> 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.

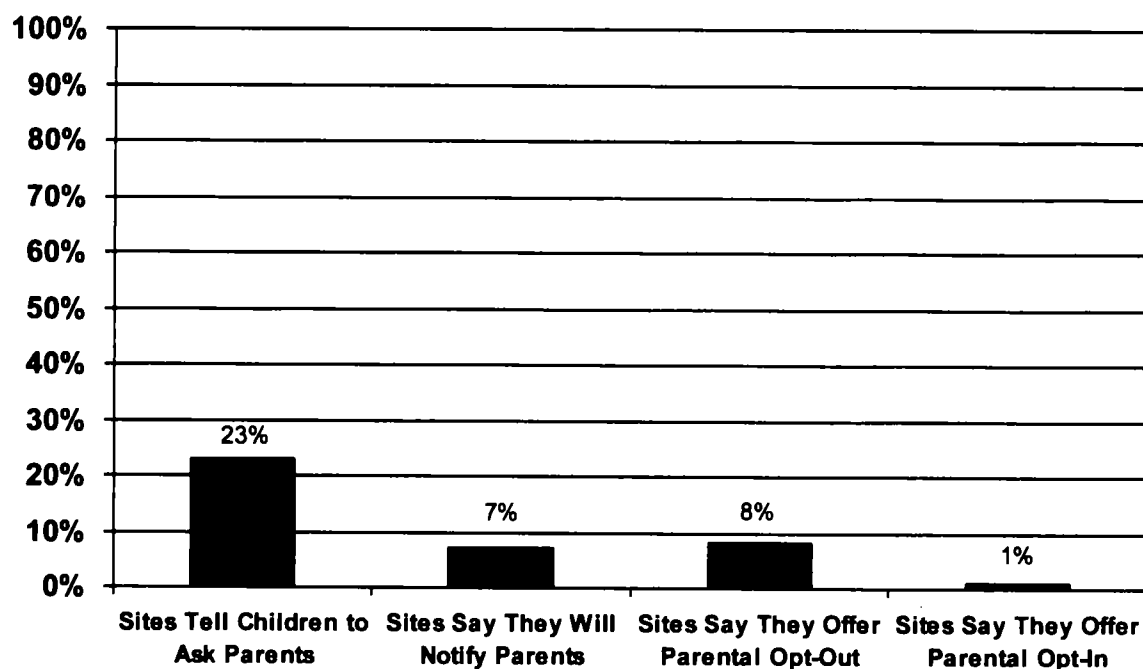
Of those sites that collect personal information from children and have an information practice disclosure, 82% have some kind of disclosure stating whether or not children's information will be publicly posted or otherwise shared with third parties.<sup>152</sup> Only 33% have an information practice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

#### **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.<sup>155</sup> Less than 8% of the sites say they notify parents of their information practices.<sup>156</sup> Only 1% (or 3 sites) require parental consent to the collection and use of information *before* the information is collected or used (opt-in)<sup>157</sup> 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).<sup>158</sup>

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.<sup>159</sup> Second, despite the fact that Commission staff publicly disclosed that the Children's Sample would be selected from sites listed in the Yahoooligans! 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.<sup>160</sup> The Federal Trade Commission Act (the "FTC Act" or "Act")<sup>161</sup> 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.<sup>162</sup> 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).<sup>163</sup>

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](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 Guidelines* 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 Yahoo!igans! 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.

## Fact Sheet # 18: Privacy In Cyberspace

---

Copyright 1995, 1996, 1997. Utility Consumers' Action Network.

June 1995 / Revised March 1997.

This copyrighted document may be copied and distributed for nonprofit, educational purposes only. The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse. This fact sheet should be used as an information source and not as legal advice. PRC materials are designed primarily for California residents. Laws in other states may vary. This publication was developed under the auspices of the University of San Diego.

---

### **Privacy Rights Clearinghouse**

5384 Linda Vista Rd. #306

San Diego, CA 92110

Voice: (619) 298-3396

Fax: (619) 298-5681

E-mail: [prc@privacyrights.org](mailto:prc@privacyrights.org)

<http://www.privacyrights.org>

---

## **Privacy In Cyberspace: Rules of the Road for the Information Superhighway**

If you have access to a computer and a modem, then you are licensed to drive on the information superhighway. And you are one of a growing number of online participants. According to one study, over one-third of the nation's households now have a personal computer. Another study found that at least 24 million people in the U.S. and Canada have used the Internet.

The information superhighway can bring many benefits to our daily lives. Unfortunately, it may create many new threats to our personal privacy as well. Unless you know the privacy "rules of the road," your online activity may lead to significant privacy problems.

If you are new to online communications, turn directly to page 7 of this fact sheet for a list of online privacy terms. Otherwise, read on.

### **What are "online communications?"**

"Online communications" are communications over telephone or cable networks using computers. Examples of online communications include connecting to the Internet through an Internet Service Provider (ISP), connecting to a commercial online service such as America Online, Compuserve, or Prodigy, or dialing into a computer bulletin board service (BBS). Increasingly, the differences between ISPs, the commercial services, and BBSs are blurring. The larger commercial services and many BBSs now provide Internet access.

The Internet raises some unique privacy concerns. Information sent over this vast network may pass through dozens of different computer systems on the way to its destination. Each of these systems may be managed by a different system operator ("sysop"), and each system may be capable of capturing and

managed by a different system operator ( sysop ), and each system may be capable of capturing and storing online communications. Furthermore, the online activities of Internet users can potentially be monitored, both by their own service provider and by the sysops of any sites on the Internet which they visit.

ISPs, commercial services, and BBSs are managed by sysops who may have different attitudes toward online privacy. Additionally, there are a tremendous variety of activities provided by all types of online services, each of which may raise specific privacy concerns.

### **What level of privacy can I expect in my online activity?**

Often the level of privacy you can expect from an online activity will be clear from the nature of that activity. Sometimes, however, an activity that appears to be private may not be. *There are virtually no online activities or services that guarantee an absolute right of privacy.*

### **Public Activities**

Many online activities are open to public inspection. Engaging in these types of activities does not normally create an expectation of privacy. In fact, according to federal law, it is not illegal for anyone to view or disclose an electronic communication if the communication is "readily accessible" to the public (Electronic Communications Privacy Act, 18 U.S.C. 2511(2)(g)(i)).

For example, a message you post to a public newsgroup or forum is available for anyone to view, copy, and store. In addition, your name, electronic mail (e-mail) address, and information about your service provider are usually available for inspection as part of the message itself. Most public postings made on the Internet are archived in searchable databases (see "For More Information," below). Thus, on the Internet, your public messages can be accessed by anyone at anytime -- even years after the message was originally written.

Other public activities may allow your message to be sent to multiple recipients. Online newsletters, for example, are usually sent to a mailing list of subscribers. If you wish to privately reply to a message posted in an online newsletter, be sure you address it specifically to that person's address, not to the newsletter address. Otherwise, you might find that your message has been sent to everyone on the newsletter mailing list.

You should not expect that your service account information will be kept private. Most services provide online "member directories" which publicly list all subscribers to the service. Some of these directories may list additional personal information. Even individuals with direct Internet accounts may be identified

| | | | | | |

### **e i Private ctivities**

may list additional personal information. Even individuals with direct Internet accounts may be identified with commands such as "finger," which let anyone with Internet access find out who else is online. Most service providers will allow users to have their information removed from these directories upon request. Be aware that some service providers may sell their membership lists to direct marketers.

"S m - " A

Often the presence of security or access safeguards on certain forums or services can lead users to believe that communications made within these services are private. For example, some bulletin board services maintain forums that are restricted to users who have a password. While communications made in these forums may initially be read only by the members with access, there is nothing preventing those members from recording the communications and later transmitting them elsewhere.

One example of this kind of behavior is the well-known "chat" conferences in which participants have been

One example of this kind of activity is the real-time "chat" conference, in which participants type live messages directly to the computer screens of other participants. Often these activities are described as private by the service provider. However, chatline users may capture, store, and transmit these communications to others outside the chat service. Additionally, these activities are subject to the same monitoring exceptions which apply to "private" e-mail (see next section).

### **"Private" Services**

Virtually all online services offer some sort of "private" activity which allows subscribers to send personal e-mail messages to others. The federal Electronic Communications Privacy Act (ECPA) makes it unlawful for anyone to read or disclose the contents of an electronic communication (18 U.S.C. 2511). This law applies to e-mail messages.

However, there are three important exceptions to the ECPA.

- ☐ The online service may view private e-mail if it suspects the sender is attempting to damage the system or harm another user. However, random monitoring of e-mail is prohibited.
- ☐ The service may legally view and disclose private e-mail if either the sender or the recipient of the message consents to the inspection or disclosure. Many commercial services require a consent agreement from new members when signing up for the service.
- ☐ If the e-mail system is owned by an employer, the employer may inspect the contents of employee e-mail on the system. Therefore, any e-mail sent from a business location is probably not private. Several court cases are pending which could affect whether or not work-related e-mail messages can be considered private. (See PRC fact sheet number 7, "Employee Monitoring: Is There Privacy in the Workplace?")

Once a sysop has intercepted e-mail for any of these lawful reasons, the sysop generally may not disclose the contents to anyone other than the addressee. Certain exceptions to this disclosure prohibition exist. These exceptions include when any party to the message consents to disclosure, when disclosure is ordered by a court, or when the message appears to involve the commission of a crime (in which case disclosure is limited to the appropriate law enforcement officials).

A sysop does not violate the ECPA if the message is accidentally sent to the wrong person. (However, the sysop may be responsible for damages caused by negligence in operating the service.)

### **Can online services track and record user activity**

| | | | | | |

Law enforcement officials may access or disclose electronic communications only after receiving a court-ordered search warrant. Only certain officials may apply for this order, and a detailed procedure is set forth in the ECPA for granting the order (18 U.S.C. 2516-2518). These provisions are relaxed for messages that have been stored in a system for over 180 days (18 U.S.C. 2703).

Remember. Your e-mail message may be handled by several different online services during delivery. The sysop of each of these systems may view e-mail under the above exceptions to the ECPA. Additionally, the message may be intercepted if either the sender or recipient consents. So, even if you do not consent yourself, the person you sent the e-mail to may have consented to the disclosure of the message.

**k d d m ?**

In a word, yes. Many types of online activities do not involve sending e-mail messages between parties. Internet users may retrieve information or documents from sites on the World Wide Web (WWW), or from "gopher" or "ftp" sites. Or users may simply "browse" these services without any other interaction.

Many users expect that such activities are anonymous. They are not. It is possible to record many online activities, including which newsgroups or files a subscriber has accessed and which Web sites a subscriber has visited. This information can be collected both by a subscriber's own service provider and by the sysops of remote sites which a subscriber visits.

Many kinds of Web-browsing software deposit on your hard drive information called "cookies," about your visit to that site. When you return to that site, "cookies" will read your hard drive to find out if you have been there before. (See page 8 for more information about "cookies" filters.)

Records of subscriber "browsing patterns," also known as "transaction-generated information," are a potentially valuable source of revenue for online services. This information is useful to direct marketers as a basis for developing highly targeted lists of online users with similar likes and behaviors. It may also create the potential for "junk e-mail" and other marketing uses. Additionally, this information may be embarrassing for users who have accessed sensitive or controversial materials online.

The practice of collecting browsing patterns is increasing. Online users should be aware that this practice poses a significant threat to online privacy. It is a good idea to contact the service provider and ask whether this type of information is collected on the system. Additionally, online users should educate themselves about what information is transmitted to remote computers by the software that they use to browse remote sites. Most World Wide Web browsers invisibly provide Web site operators with information about a user's service provider, and with information about the location of other Web sites a user has visited. Some Web browsers are programmed to transmit a user's e-mail address to each Web site a user visits.

Users who access the Internet from work should know that employers are increasingly monitoring the Internet sites which an employee visits. Be sure to inquire about your employer's online privacy policy. If there is none, recommend that such a policy be developed.

In order for law enforcement officials to gain access to subscriber transactional records, they must obtain a court order demonstrating that the records are relevant to an ongoing criminal investigation

**Can an online service access information stored in your computer without your knowledge**

|  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**What can you do to protect your privacy in cyberspace**

(Communications Assistance for Law Enforcement Act, 18 U.S.C. 2703(d)). This provision prevents "fishing expeditions" by government officials, hoping to find evidence of crimes by accident.

**f m d m m m k d ?**

Unfortunately, the answer to this question is yes. Many of the commercial online services will automatically download graphics and program upgrades to the user's home computer. News reports have documented the fact that certain online services have admitted to both accidental and intentional "prying" into the memory of home computers signing on to the service. In some cases, personal files have been copied and collected by the online services.

It is difficult to detect these types of intrusions. The online user should be aware of this potential privacy abuse, and investigate new services thoroughly before signing on. Always ask for the privacy policy of any online service you intend to use.

**W I d m b ?\***

When you are sitting alone at your computer, "surfing" the Internet, sending electronic mail messages and participating in online forums, it's easy to be lulled into thinking that your activities are private. Be aware that at any step along the way, your online messages could be intercepted, and your activities monitored,

in the vast untamed world of cyberspace.

1. Your account is only as secure as its **password**. Create passwords with nonsensical combinations of upper and lower case letters, numbers and symbols, for example tY8%uX. Change your password frequently. Never write it down or give it to someone else. Don't let others watch you log in. Never leave your computer logged in unattended.

2. Contact the sysop of any online service you intend to use and ask for its **privacy policy**. Most of the commercial services have written privacy policies which are provided to new subscribers. Also, carefully read all messages which appear on initial login. Many sysops notify online users in login messages that e-mail is subject to inspection. Many services require new subscribers to allow e-mail to be monitored as part of the sign-up process. All sysops should have a well-defined, written policy concerning privacy. Those that do not should be avoided.

3. **Shop around**. Investigate new services before using them. A good way to do this is to post a question about a new service in a dependable forum or newsgroup. Bad reputations get around quickly in cyberspace, so if others have had negative experiences with a service, you should get the message.

4. Assume that your online communications are **NOT private** unless you use powerful encryption. Do not send sensitive personal information (phone number, password, address, credit card number, vacation dates) by chat lines, forum postings, e-mail or in your online biography.

5. Be cautious of "**start-up**" **software** that makes an initial connection to the service for you. Often these programs require you to provide credit card numbers, checking account numbers, Social Security numbers, or other personal information, and then upload this information automatically to the service. Also, these programs may be able to access records in your computer without your knowledge. Contact the service for alternative subscription methods.

6. Note that public postings made on the Internet are often **archived** and saved for posterity. For example, it is possible to search and discover the postings an individual has made to Usenet newsgroups. (See information about the search tools [DejaNews](#) and [Alta Vista](#) below.) This information can be used to create profiles of individuals for a variety of purposes, such as employment background checks and direct marketing.

## electronic footprints

## favorite newsgroups

## delete cookies

## online identities

**7** Be aware that online activities leave **f** for others to see, both at your own service provider and at any remote sites you visit. Your own service provider can determine what commands you have executed and track which sites you visit. Web site operators can often track the activities you engage in on their site, particularly at sites which ask you to "register" or otherwise provide personal information. Some Web browsing software transmits less information to remote sites than other software. You can avoid leaving tracks when you send e-mail messages by using anonymous remailers. (See pages 6 and 8 for information about remailers.)

**8** If your online service allows you to compile a list of **f**, or lets you arrange newsgroups by priority, be aware that your sysop can monitor that list. Do not place controversial or sensitive newsgroups in this list if you want to avoid being connected to particular issues.

**9** The "**d**" **mm** **d** does not make your messages disappear. They can still be retrieved from back-up systems.

**10** Be aware that others' **d** are not always what they seem. Many network users adopt

### online identities

one or more online disguises.

**11. Your online biography**, if you create one, may be searched system-wide or remotely "fingered" by anyone. If for any reason you need to safeguard your identity, don't create an online "bio". Ask the system operator of your service to remove you from its online directory.

**12. If you publish information on a personal Web page**, note that direct marketers and others may collect your address, phone number, and any other information that you provide.

**13. Be aware of the possible social dangers** of being online: harassment, stalking, being "flamed" (emotional verbal attacks), or "spamming" (being sent frequent unsolicited messages). Women can be particularly vulnerable if their e-mail addresses are recognizable as women's names. Consider using gender-neutral online IDs.

**14. If your children** are online users, teach them about appropriate online privacy behavior. Caution them against revealing information about themselves or your family. (See below.)

**15. Take advantage of privacy protection tools.** There are several technologies which help online users protect their privacy. Discussed here are **encryption, anonymous remailers and memory protection software.**

**Encryption.** Encryption is a method of scrambling an e-mail message or file so that it is gibberish to anyone who does not know how to unscramble it. The privacy advantage of encryption is that anything encrypted is virtually inaccessible to anyone other than the designated recipient. Thus, private information may be encrypted, and then transmitted, stored or distributed without fear that it will be scrutinized by outsiders.

An encrypted e-mail message cannot be read by the online service sysop, or anyone else who has obtained the message legally or illegally. Therefore, any message containing private or sensitive information should be encrypted prior to communicating it online. Various strong encryption programs, such as PGP (Pretty Good Privacy) are available online. (See below for details.)

Because encryption prevents unauthorized access, law enforcement agencies have expressed concerns over the use of this technology, and Congress has considered legislation to create a "back door" to allow law enforcement officials to decipher encrypted messages. Users should be aware that the legal status of

### anonymous remailers

### memory protection software

this technology is still unsettled. Moreover, it is against the law to export encryption technology to other countries (International Traffic in Arms Regulations, 22 CFR 120.1 et seq.). However, its use within the United States is not currently restricted.

**A n o n y m o u s .** Because it is relatively easy to determine the name and e-mail address of anyone who posts messages or sends e-mail, the practice of using anonymous remailing programs has become more common. These programs receive e-mail, strip off all identifying information, then forward the mail to the appropriate address. There are several anonymous servers available on the Internet. (See below for more information.)

**M o n i t o r i n g s o f t w a r e .** Software security programs are now available which help prevent unauthorized access to files on the home computer. For example, one program encrypts every directory with a different password so that to access any directory you must log in first. Then, if an online service provider tries to read any private files, it would be denied access. These programs may include an "audit trail" that records all activity on the computer's drives

that they record an activity on the computer's screen.

## Glossary of Online Terms

**BBS** - Stands for Bulletin Board System. A local computer that can be called directly with a modem. Usually they are privately operated, and offer various services depending on the owner and the users. Often a BBS is not connected to a network of other computers, but increasingly BBSs are offering Internet access.

**Commercial Online Service** - A service in which users pay a certain fee to dial into what is essentially a very large BBS. These services provide a wide range of conferences, forums, software files, news and information, as well as e-mail service. Examples include Prodigy, CompuServe, America Online, the Microsoft Network, and others. Many of these services offer at least limited access to the Internet.

**Cookies** - A feature of many Web browsers defined as client-side persistent information. Cookies allow Web sites to store information about your visit to that site on your hard drive. Then, when you return, cookies will read your hard drive to find out if you have been there before.

**Cyberspace** - The "place" where online activities occur. Commentators have noted that many of the activities that take place online are analogous to activities that occur in physical space. These online activities are said to take place in cyberspace.

**FTP** - Stands for File Transfer Protocol. A system of file storage on the Internet that allows users to upload or download entire files.

**Gopher** - A software program that archives files of information and displays the files in an organized directory which may be accessed via the Internet. These archives are called "gopher sites." Named after the University of Minnesota mascot, the golden gophers, where the software was developed. Gopher sites are being replaced by Web sites (see below).

**Internet** - An immense global network of computers. The Internet is not owned by any one entity, but rather owners of individual computer systems agree to participate in it. Users with an account with one of these computers generally may connect with any other computer on the network.

**ISP** - Stands for Internet Service Provider. A service which provides subscribers with direct access to the Internet. Some of the larger ISPs include Netcom, Pipeline, and Panix. Many small, local ISPs exist.

o e

ewsgroups

nline

R

|

|

||

|

|

Internet. Some of the larger ISPs include Procom, Tropic, and T-Online. Many smaller, local ISPs exist.

**M d m** - Acronym for modulator/demodulator. Equipment which converts the digital signals of your computer (the '1s' and '0s') into analog signals which can be transmitted over the telephone network, and vice-versa.

**N** - Newsgroups are lists of messages from users grouped by specific topics. Usenet is a network of thousands of these electronic conferences which may be accessed on the Internet. Most commercial services and BBSs have similar public forums.

**O** - Connected to a computer network.

**U L** - Stands for Universal Resource Locator. URLs are unique addresses assigned to every location on

## R

the Internet. URLs for Web pages begin with the letters "http."

**WWW** - Stands for World Wide Web. This powerful tool for accessing the Internet combines graphics, "point and click" navigation commands, and a method of linking many different sites to allow users to quickly and easily search for information on the Internet.

**Web page** - A location on the World Wide Web which can be visited by Internet users employing software called a Web browser. Every Web page is identified by a unique address, called a URL. Publishing information on a Web page is a relatively simple and low-cost process. A collection of related Web pages maintained on a single computer system, or sometimes just a single Web page, comprises a Web site.

## For More Information

Several **public interest groups** advocate on behalf of online users. They also have extensive information about privacy issues available via their online archives.

- ❑ **Center for Democracy and Technology**, 1634 I St. N.W. #1100, Washington, DC 20006. Voice: 202-637-9800 Fax: 202-637-0968 E- mail: [info@cdt.org](mailto:info@cdt.org) URL: <http://www.cdt.org>
- ❑ **Computer Professionals for Social Responsibility**, P.O Box 717, Palo Alto, CA 94302. Voice: 415-322-3778 Fax: 415-322-4748 E- mail: [cpsr@cpsr.org](mailto:cpsr@cpsr.org) URL: <http://www.cpsr.org>
- ❑ **Electronic Frontier Foundation**, 1550 Bryant Street #725, San Francisco, CA 94103. Voice: 415-436-9333 Fax: 415-436-9993 E- mail: [eff@eff.org](mailto:eff@eff.org) URL: <http://www.eff.org>
- ❑ **Electronic Privacy Information Center**, 666 Pennsylvania Ave. SE #301, Washington, DC 20003. Voice: 202-544-9240 E-mail: [info@epic.org](mailto:info@epic.org) URL: <http://www.epic.org>
- ❑ **NetAction**, 601 Van Ness Ave. #631, San Francisco, CA 94102. Voice: 415-755-8674. E-mail: [akrause@igc.org](mailto:akrause@igc.org) / URL: <http://www.netaction.org>

Several **online newsletters** discuss cyberspace privacy issues:

- ❑ *Computer Privacy Digest*: CPD can be read as a Usenet newsgroup, [comp.society.privacy](mailto:comp.society.privacy). Alternatively, to receive CPD via e-mail, send a request to the newsletter's moderator at: [comp-privacy-request@uwm.edu](mailto:comp-privacy-request@uwm.edu)
- ❑ *Privacy Forum*: For subscription information, send an e-mail message consisting of the word "help" (without quotes) in the *body* of the message to: [privacy-request@vortex.com](mailto:privacy-request@vortex.com)

To see a **demonstration** of the kind of information that can be compiled about you when you surf the Web, visit the site of the **Center for Democracy and Technology**: <http://www.cdt.org>

cookies      loggers

---



---



---

This site also has information about "cookies." And it lists the privacy policies of the major online service providers: AOL, CompuServe, Msnet, and Prodigy.

To learn more about "k", "b", and other types of online filters, visit these Web sites:

- ☐ <http://www.privnet.com>
- ☐ <http://www.wizvax.net/kevinmca/>

To learn more about anonymous Web browsing, visit the Web site:

- ☐ <http://www.anonymizer.com>

To see some examples of the powerful **search tools** available to find public postings made on the Internet, visit the following Web sites:

- ☐ Alta Vista at <http://www.altavista.digital.com>
- ☐ DejaNews at <http://www.dejanews.com>

To learn more about the **encryption** program PGP, contact these online sources:

- ☐ "Where to Get PGP," compiled by Michael Paul Johnson. <ftp://ftp.csn.net/mpj/getpgp.asc>
- ☐ "PGP Frequently Asked Questions with Answers," compiled by Jeff Licquia.  
<http://www.prairienet.org/~jalicqui/pgpfaq.txt>

For information about **anonymous remailers**, the following online resource is helpful:

- ☐ "Anonymous Remailers FAQ," compiled by Andre Bacard.

If your **children are online users**, request the free brochure, "Child Safety on the Information Highway," from the National Center for Missing and Exploited Children. Voice: 800-843-5678.

You may learn more about "parental control" software programs by visiting the following sites. These online filters both limit the types of sites children can visit and prohibit online users from disclosing certain information, like names and address.

- ☐ Cyber Patrol: <http://www.microsys.com>
- ☐ Cyber Sitter: <http://www.solidoak.com>
- ☐ N2h2: <http://www.n2h2.com>
- ☐ Net Blocker: <http://www.netblocker.com>
- ☐ Net Nanny: <http://www.netnanny.com/netnanny>
- ☐ Surf Watch: <http://www.surfwatch.com>

The major **federal and state laws** affecting online privacy are:

- ☐ The federal Electronic Communication Privacy Act of 1986, 18 U.S.C. 2511 et seq.
- ☐ California Penal Code 631 et seq., regarding wiretapping and recording telephone messages (known as the Invasion of Privacy Act).

The resources of the **Privacy Rights Clearinghouse** are available online:

- ☐ URL: <http://www.privacyrights.org>
- ☐ E-mail: [prc@privacyrights.org](mailto:prc@privacyrights.org)

---

**HOME**

## **Description of "Alliance for Online Consumer Awareness"**

Department of Commerce, April 6, 1998

*Privacy*

A coalition of U.S. businesses, lead by IBM, proposes to create a self-regulatory umbrella group to promote compliance with fair information practices on the Internet. The group intends to "preview" the initiative in May (at the DOC privacy event), with a commitment to begin operations in September, 1998. At this point, the composition of the alliance has not gelled. We understand that AT&T, EDS, Hewlett-Packard, and a number of other businesses are in discussion with IBM.

The alliance proposes to work with business, consumer groups and privacy advocates to create an "accountability mechanism" available to any consumer in connection with any online encounter. The organization would provide:

- support for fair information practices including awareness, choice, security, access and accuracy;<sup>1</sup>
- business education and encouragement of companies and associations to promulgate and post privacy guidelines and/or policies developed on sectoral basis by individual business sectors;
- consumer outreach and consumer education about privacy rights and how to protect personal privacy online;
- resolution of "legitimate" consumer complaints;
- verification, as appropriate, of business compliance with stated privacy policies;
- consequences for businesses that fail to adhere to stated practices (investigation and disclosure of noncompliance, revocation of alliance seal, referral to consumer protection agencies when complaints are not resolved through private dispute resolution mechanisms).

In addition to general support for fair information practices, the alliance proposes to

---

<sup>1</sup> In general, the alliance would enforce privacy policies developed on a sectoral basis. The alliance would require, however, that all policies comply with the fair information practices guidelines established by the OECD in 1980. The alliance believes that some evolutionary period will be needed, however. For example, some time may be needed to reach agreement on consumer access to their personal data.

The alliance would also require members to comply with specific rules relating to the collection of data from children. Alliance members are discussing appropriate rules governing the collection of data from children. We believe that these rules should, at a minimum, provide the protections outlined in FTC staff guidance on the subject.

focus on consumer education (to increase awareness) and on accountability.

To promote consumer awareness and empowerment, the alliance would publish basic educational materials about online privacy. For example, the alliance would provide what they should consider before disclosing personal information. the alliance would provide training on the use of consumer empowerment technology. It would create a digital seal (like the "Good Housekeeping Seal of Approval") to encourage consumers to do business with companies that adhere to fair information practices. The alliance would also make information available about non-compliance, based on verified complaints about personal data protection practices.

To enhance business accountability for inappropriate use of personal data, the alliance would provide a hotline/hotsite to respond to consumer inquiries about online privacy and suspected violation of fair information practices. The alliance would help businesses develop privacy policies, and if a company chooses, permit a company to display an alliance seal that assures consumers that a particular online business complies with fair information practices. The alliance would audit or otherwise assess member company compliance.<sup>2</sup> Finally, the alliance would handle consumer complaints about privacy violations.

The coalition is currently discussing a partnership with BBBOnLine, a subsidiary of the national Council of Better Business Bureaus. Under this model, BBBOnLine would provide a competitor challenge and consumer complaint resolution service, including mediation and arbitration using the existing BBB dispute settlement apparatus.

The alliance is also current discussing a partnership with TRUSTe, an organization that provides trust marks (seals), backed by independent audits and third party verification (list seeding, etc.).

The details of the alliance proposal are still under discussion with founding members. The proposal appears, however, to have the elements that we believe are necessary to create effective self-regulation for privacy.

---

<sup>2</sup> The use of independent audits and/or other independent assessment mechanisms remains controversial. Traditional financial audits are quite expensive and may not be necessary in all cases. While we are willing to consider other approaches, we believe that independent assessment of adherence with fair information practices is a critical element of any self-regulatory approach to data privacy.

FOR RELEASE: March 26, 1998

---

**FTC PRESENTS TESTIMONY TO CONGRESS  
ON INTERNET PRIVACY**

The Federal Trade Commission's Associate Director for Credit Practices, David Medine today presented Commission testimony on Internet privacy to the House Judiciary Subcommittee on Courts and Intellectual Property.

Over the past three years, the FTC has been examining the personal privacy and consumer protection issues raised by the collection and use of information about consumers as they use the Internet. A number of public workshops have been held by the agency's Bureau of Consumer Protection. Throughout the workshops, the online industry has advocated self-regulation as the most efficient and effective means of creating online privacy protections. This month, FTC staff is conducting a survey of 1,200 commercial Web sites to determine the extent to which these sites, including sites directed to children, are disclosing how they collect and use personal information online. The Commission will be submitting a report to Congress in June on the effectiveness of self-regulatory approaches to protecting consumers' privacy online.

The Commission's testimony outlines the agency's focus on individual reference services, unsolicited commercial E-mail, and online information collection practices relating both to adults and children. It points to the Commission's efforts to encourage online firms to address consumer concerns through self-regulation. The testimony states that the "Commission recognizes the importance of the development of the Internet as a viable and safe marketplace for consumers." The FTC's efforts over the last few years have shown that the online marketplace likely will not flourish until sufficient privacy protections are implemented online. The report to Congress will disclose the results of the staff's Web survey and will analyze how much progress self-regulation has made in achieving effective online privacy protections for consumers, the testimony notes. "If such progress is inadequate, appropriate alternatives may need to be explored," the testimony concludes.

The Commission vote to authorize the testimony was 5-0.

---

**Copies** of the testimony as well as transcripts of FTC workshops on Internet privacy, a Commission staff report titled, "Consumer Privacy on the Global Information Infrastructure," a Commission report on individual reference services as well as public commentary submitted for the workshops and prior press releases on Internet privacy issues are **available** on the FTC's web site at <http://www.ftc.gov> and also from the FTC's Consumer Response Center; 202-326-3128; TDD for the hearing impaired 202-326-2502. To find out the latest news as it is announced, call the FTC NewsPhone recording at 202-326-2710.

**MEDIA CONTACT:**

Victoria Streitfeld  
Office of Public Affairs  
202-326-2718

**STAFF CONTACT:**

David Medine  
Bureau of Consumer Protection  
202-326-3224

(FTC File No. 954 807)

(inhouse)

**PREPARED STATEMENT OF THE  
FEDERAL TRADE COMMISSION ON**

**"INTERNET PRIVACY"**

**Before the**

**SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY  
of the  
HOUSE COMMITTEE ON THE JUDICIARY  
UNITED STATES HOUSE OF REPRESENTATIVES  
Washington, D.C.**

**March 26, 1998**

---

Mr. Chairman and members of the House Judiciary Committee: I am David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of privacy on the Internet.<sup>(1)</sup>

**I. Introduction**

***A. Internet Privacy***

The Internet is an exciting new marketplace for consumers. It offers not only easy access to a vast array of goods and services, but also to rich sources of information that enable consumers to make better-informed purchasing decisions.

The online consumer market is growing exponentially. In early 1997, 51 million adults were already online in the U.S. and Canada.<sup>(2)</sup> Of those people, 73% reported that they had shopped for product information on the World Wide Web ("the Web"), the interactive graphics portion of the Internet.<sup>(3)</sup> 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.<sup>(4)</sup> Further, analysts estimate that Internet advertising -- which totaled approximately \$301 million in 1996 -- will swell to \$4.35 billion by the year 2000.<sup>(5)</sup>

These figures suggest rapid growth of the online marketplace, but there are also indicators 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 online merchants handle personal information than they have in how traditionally off-line institutions, such as hospitals and banks, handle such information.<sup>(6)</sup> 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.<sup>(7)</sup> According to the results of a *Business Week* survey released earlier this month, 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.<sup>(8)</sup> These findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until sufficient consumer privacy protections are implemented in the online marketplace.

***B. The FTC's Role***

The mission of the FTC is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission undertakes this mission by enforcing the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.<sup>(9)</sup> The Commission's responsibilities are far-reaching. With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector in our economy.<sup>(10)</sup> Commerce on the Internet falls within the scope of this statutory mandate.

### ***C. The FTC's Approach to Online Privacy***

The Commission is taking a proactive approach to online privacy issues impacting consumers by: (1) identifying potential consumer protection issues related to online marketing and commercial transactions; (2) providing a public forum for the exchange of ideas and presentation of research and technology; and (3) encouraging self-regulation.

The Commission's first public workshop on privacy was held in April 1995. In a series of hearings held in October and November 1995, the FTC examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. 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*. The agency held a four-day workshop in June 1997 to explore issues raised by computerized databases that contain consumers' personal identifying information (also known as "individual reference services" or "look-up" services). This workshop also explored issues relating to unsolicited commercial e-mail, online privacy, and children's online privacy.

These FTC 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. Further, the Commission and its staff have issued reports describing various consumer privacy concerns in the electronic marketplace.<sup>(11)</sup> In addition, FTC staff has written opinion letters delineating what types of practices in this area might violate the Federal Trade Commission Act.<sup>(12)</sup>

## **II. Focus of FTC Privacy Activities**

Following the June 1997 workshop, the Commission focused on a number of key privacy issues impacting consumers. These issues were discussed in a July 31, 1997, letter (Attachment A) responding to a joint request from Chairman John McCain and Chairman Tom Bliley for a brief report on the Commission's findings from the workshop. The Commission's letter summarized its work and provided a plan to address concerns raised by the following issues: (1) computerized databases containing consumers' personal identifying information, *i.e.*, individual reference services or look-up services; (2) unsolicited commercial e-mail; (3) online information collection; and (4) children's privacy in the online environment. I will address each of these issues today. In addition, as set forth in the July 31 letter, the Commission intends to issue a report to Congress in June 1998 that will focus on the Commission's efforts to monitor and assess the status of self-regulatory efforts by industry members involved in the online collection and dissemination of consumer information.

### ***A. Individual Reference Services***

In response to growing public and Congressional concern, the Commission examined the availability of sensitive personal identifying information through computerized database services that are used to locate, identify, or verify the identity of individuals, often referred to as individual reference services or look-up services. The Commission's study of look-up services culminated in a report to Congress in December 1997. The report summarized what the Commission had learned about the individual reference services industry; examined the benefits, risks, and potential controls associated with these services; assessed the viability of an industry self-regulatory proposal; and concluded with recommendations that address concerns left unresolved by the proposal.<sup>(13)</sup>

The Commission found that a vast amount of information about consumers is available to customers of individual reference services through the services' proprietary computer networks and increasingly over the Internet. Gleaned from various public and proprietary sources, information available through the services ranges from purely identifying information, *e.g.*, name and phone number, to much more extensive data, *e.g.*, driving records, criminal and civil court records, property records, and licensing records.<sup>(14)</sup> The Commission also learned that convenient access to this type of information confers a myriad of benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, parents to find missing children, journalists to report the news, and consumers to find lost relatives.<sup>(15)</sup> At the same time, the increasing availability of this information poses various risks of harm to consumers' privacy and financial interests, including the possibility of increasing the incidence of identity theft.<sup>(16)</sup>

At the June 1997 workshop, a group of industry members (the "Individual Reference Services Group" or "IRSG") announced its intent to address concerns associated with its industry through self-regulation. Commission staff worked with this group to encourage it to adopt an effective self-regulatory program. In December 1997, 14 companies, a substantial majority of the individual reference service industry, agreed to abide by the "IRSG Principles," a set of principles that addresses the availability of information obtained through individual reference services.

The IRSG Principles restrict access to certain information obtained from "non-public" sources contained in each signatory's database. This non-public information includes what is called "credit header" information, which is that portion of a credit report purchased from a credit reporting agency that contains an individual's name, address, aliases, Social Security number, current and prior addresses and telephone number.<sup>(17)</sup> The restrictions vary according to the category of customer. Customers that have less restricted access to non-public information are subject to greater controls. It is noteworthy that the IRSG Principles prohibit distribution to the general public -- over the Internet or otherwise -- of certain non-public information, including Social Security number, mother's maiden name, and date of birth. In addition, consumers will be able to access the non-public information maintained about them in these services and to prevent the sharing (*i.e.*, "opt out") of the non-public information distributed to the general public.<sup>(18)</sup>

The IRSG Principles show particular promise because they include a compliance assurance mechanism and are likely to influence virtually the entire individual reference services industry. First, signatories must undergo an annual compliance review by a professional third party such as an accounting firm, the results of which will be made public. Public examination of the results of compliance reviews and the possibility of liability under the FTC Act and similar state statutes should create an incentive for compliance by signatories. Second, signatories that are information suppliers (*e.g.*, the three national credit reporting agencies) are prohibited from selling information to entities

whose practices are inconsistent with the Principles. Therefore, non-signatories whose practices are inconsistent with the Principles likely will be unable to obtain non-public information easily for redissemination through their services. Thus, the IRSG Principles should substantially lessen the risk that information held by these services will be misused, and they should address consumers' concerns about the privacy of their non-public information.<sup>(19)</sup>

The Commission concluded that the IRSG Principles address many of the concerns associated with the increased availability of non-public information through individual reference services while preserving important benefits conferred by this industry. However, important issues related to individual reference services remain. For example, the IRSG Principles do not give consumers access to the "public information" (e.g., real estate, motor vehicle, and court records) maintained about them and disseminated by the look-up services. Accordingly, consumers will not be able to check for inaccuracies resulting from transcription or other errors occurring in the process of obtaining or compiling the public information by the look-up services. IRSG members have agreed to revisit this issue by June 1999, and to consider whether to conduct a study quantifying the extent of any such inaccuracies. The Commission has urged the IRSG to conduct an analysis to determine whether the frequency of inaccuracies and the harm associated with them are such that consumer access to public record information or other safeguards are in fact unnecessary.<sup>(20)</sup>

In its report to Congress, the Commission also encouraged public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices. Finally, the Commission has acknowledged and encouraged the ongoing efforts of many privacy advocates, consumer groups, government agencies, and the IRSG to educate the public about information privacy issues.<sup>(21)</sup>

### ***B. Unsolicited Commercial E-mail***

At the 1997 Workshop, the Commission also gathered a considerable body of information concerning the problem of unsolicited commercial e-mail ("UCE"). Three UCE-related initiatives grew out of that workshop. First, a cross-section of interested parties, including Internet service providers, online firms, senders of UCE, and privacy advocates, formed a working group to develop a self-regulatory solution to the problems associated with UCE. This group, which has been led by the Center for Democracy and Technology, a non-profit, public interest organization involved in new technology issues, is expected to issue a report outlining proposed solutions. Second, the Commission brought enforcement actions against scam artists who make allegedly fraudulent solicitations via UCE,<sup>(22)</sup> and continues to investigate other possible frauds committed through UCE. Third, the Commission has launched an educational campaign. Staff have produced educational materials warning consumers to be suspicious of the solicitations they receive in UCE and are distributing them through channels designed to reach those who are likely to use e-mail. Staff also monitored thousands of UCE messages, identified those which appeared facially deceptive, and sent letters to over one thousand senders of these UCE messages, advising them of the legal requirements applying to their activities.

### ***C. Online Information Collection Practices***

Many consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections.<sup>(23)</sup> During the Commission's first privacy workshop, a consensus emerged among workshop participants regarding four important considerations that would assist in protecting online privacy. These considerations include: **notice** concerning Web sites' information practices, *i.e.*, how commercial Web sites will use personal information they collect from consumers;

**choice** in how Web sites will use consumers' personal information; **access** to consumers' own information collected, maintained, or used by Web sites; and **security** of consumers' personal information maintained by Web sites from improper or unauthorized use by third parties.<sup>(24)</sup>

### **1. Commitment to Self-Regulation**

The Commission has also learned that members of the online industry are aware of the need to address consumers' concerns. Throughout the series of Commission workshops on these issues, the online industry has asserted that self-regulation is the most efficient and effective means of creating online privacy protections. Industry groups have demonstrated varying approaches to protecting online consumer privacy. As of June 1997, certain key trade associations had developed policies and procedures to protect online privacy. Others were in the initial stages of policy formation, and still others remained uncertain as to whether industry-wide policies, as opposed to individual company efforts, would be necessary. Trade association representatives committed to develop privacy policies as guidance for their members and to encourage their members to post their own information practices on their Web sites. In addition, a non-profit group called TRUSTe launched a proprietary system requiring disclosure of member Web sites' basic information practices and third-party auditing of those practices, but the system had not yet been widely implemented.<sup>(25)</sup> Its efficacy will depend upon widespread industry participation.<sup>(26)</sup>

The Commission has also learned of promising efforts to create interactive technology that permits consumers to automate their preferences, and Web sites to communicate their practices, regarding the collection and use of personal information online. At the time of the 1997 Workshop, these technological tools, which potentially could provide adequate privacy protection, were still in the initial stages of development.<sup>(27)</sup>

### **2. Online Information Collection from and about Children**

The collection of information from and about children who use the Internet deserves special attention. Internet usage by children is growing: a 1997 survey indicates that approximately 9.8 million children (under age 18) go online, which is a five-fold increase from 1995.<sup>(28)</sup> Children use the Internet for a variety of activities including homework or informal learning, playing games, browsing or for e-mail/chat rooms.<sup>(29)</sup> These young people are not shopping or banking online, but parents still have serious concerns about the online collection and use of personal information from children. A 1997 survey indicates that 97 percent of parents whose children use the Internet believe Web sites should not sell or rent personal information on children; 80 percent object to a Web site requesting a child's name and address when the child registers, even if such information is used only internally.<sup>(30)</sup>

Several workshop participants voiced concern at the 1997 Workshop about online activities that enable children to post or disclose their names, street addresses, or e-mail addresses in areas accessible to the public, such as chat rooms, bulletin boards, and electronic pen pal programs, creating a serious risk that the information may fall into the wrong hands.<sup>(31)</sup> For example, anecdotal evidence indicates that many children surfing the Internet claim to have experienced problems, such as attempted password theft and inappropriate advances by adults in children's chat rooms.<sup>(32)</sup> Further, the FBI and Justice Department's "Innocent Images" investigation reveals that online services and bulletin boards are rapidly becoming the most prevalent sources used by predators to identify and contact children.<sup>(33)</sup>

Industry guidelines on the collection and use of children's information were presented by

the Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus and by the Direct Marketing Association, among others.<sup>(34)</sup> All of the guidelines call for some form of notice and some degree of parental choice over the disclosure of personal information about children to third parties. The guidelines, however, do not always make clear what specific steps would satisfy these obligations or take into account that children may be online without parental supervision.

Overall, there was strong support at the 1997 Workshop for development of technological tools, such as filtering or browser software, to protect children's privacy. Yet, important limitations were identified, such as the ability of computer-savvy children to defeat technological protections and the fact that their widespread implementation and use may be over a year away.<sup>(35)</sup> These technologies are only now being applied to protecting privacy, and their effectiveness will depend on their widespread adoption by industry and parents.

Finally, the information presented at the 1997 Workshop demonstrated the need to educate parents about privacy issues concerning their children's use of the Internet and the need for parents to establish clear rules for children on providing information to Web sites. Commission staff is developing additional educational materials for parents and children regarding privacy protections for children online and, most importantly, looking for ways to work with affected industries, consumer groups, and educators to develop educational initiatives.<sup>(36)</sup>

### **3. Encouraging Self-Regulation**

The Commission has encouraged industry to address consumer concerns through self-regulation. In the Commission's view, self-regulation in the first instance generally is more prompt, flexible, and effective than government regulation. Further, self-regulation can bring the accumulated judgment and experience of industry to bear on issues that may be difficult for the government to define with bright-line rules. Industry and consumers are well-situated to know what is needed and where immediate concerns lie. The IRSG Principles provide one promising model for self-regulation.

Commission staff has recently issued some guidance that should strengthen self-regulatory efforts to protect consumers' privacy both online and off-line. The 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.<sup>(37)</sup>

### **4. Monitoring Self-Regulation**

The Commission continues to monitor the online collection and use of information from consumers, including children. Last October, Commission staff conducted a "Kids Privacy Surf Day," designed as a "quick snapshot" -- not a comprehensive survey -- of children's Web sites' privacy practices. Staff found that more than 80 percent of the over 100 sites surveyed were collecting personal identifying information from children, most without seeking parental permission or allowing parents to control the collection and use of the information. Commission staff sent the surveyed Web sites e-mail messages notifying them of potential law violations in connection with their information collection practices.

This month, the Commission is conducting a survey of commercial Web sites, including sites directed to children, to determine the extent to which they are disclosing their information practices and offering consumers choice regarding the online collection and use of their personal information. The survey covers approximately 1200 Web sites: 100 of the most frequently visited Web sites; roughly 900 sites drawn from a database of commercial Web sites maintained by Dun & Bradstreet, including subsamples representing the retail, health, and financial sectors; and roughly 200 children's sites drawn from Yahoo!igans' online directory of sites of interest to children. In particular, the Commission is looking at whether sites display privacy policies or discrete statements about their information practices and whether such disclosures (1) include notice to consumers as to whether their information will be transferred to third parties; (2) provide consumers with choice over the use of their information; (3) allow consumers to access the information that is maintained about them; and (4) inform consumers that security precautions will be taken to protect their information after it has been transferred. Further, the Commission is assessing whether the policies are easy to find. As to sites directed to children, the Commission is also determining whether individual sites allow parents to have control over the collection, disclosure, and use of their children's information.

### III. Report to Congress: Assessing Staff's Findings

As mentioned above, the Commission's upcoming report to Congress will focus on the effectiveness of self-regulation as a means of protecting consumer privacy online. The Commission will summarize and assess its findings from this month's comprehensive survey of commercial Web sites. The report will also include the Commission's analysis of existing industry guidelines and principles on the online collection and use of consumers' personal information. Toward that end, the Commission issued a *Federal Register* notice on March 5, 1998, requesting that interested trade associations and industry groups submit copies of their information practice guidelines and principles for inclusion in the Commission's report.

### IV. Conclusion

The Commission recognizes the importance of the development of the Internet as a viable and safe marketplace for consumers. In order for the online marketplace to grow, sufficient privacy protections must be in place. The Commission supports technological innovation and also encourages industry self-regulation so long as self-regulation proves meaningful and effective. The upcoming June report describing the results of the staff's Web survey will shed light on how much progress self-regulation has made in achieving effective online privacy protection for consumers. If such progress is inadequate, appropriate alternatives may need to be explored.

---

#### Endnotes:

1. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any one Commissioner.
2. 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) (reported at [http://www.commerce.net/work/pilot/nielsen\\_96/press\\_97.html](http://www.commerce.net/work/pilot/nielsen_96/press_97.html)) [hereafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS™)*: Second Quarter 1997 Study Sept. 4, 1997) (reported at <http://www.intelliquest.com/about/release32.htm>).
3. *CommerceNet/Nielsen Demographic Study*, Spring '97.
4. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic*

*Commerce Study*, Fall '97 (December 11, 1997) (reported 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) (reported at <http://www.yankelovich.com/pr/970327.HTM>) (finding that 23% of users ordered and paid for a product over the Internet, i.e., "transacted" business online).

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

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

7. *Id.* at 20-21.

8. "Business Week/Harris Poll: Online Insecurity," *Business Week*, March 16, 1998.

9. 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately thirty additional statutes, e.g., the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 35 rules governing specific industries and practices, e.g., the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

10. Certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2) and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

11. E.g., FTC Report to Congress: *Individual Reference Services*, December 1997; FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996; FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, May 1996. In addition, the Commission presented testimony on September 18, 1997, on the Implications of Emerging Electronic Payment Systems on Individual Privacy before the House Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services.

12. E.g., Letter from Bureau of Consumer Protection Director to Center for Media Education, July 15, 1997.

13. FTC Report to Congress: *Individual Reference Services*, December 1997.

14. *Id.* at 4-5.

15. *Id.* at 9-11.

16. *Id.* at 13-16.

17. *Id.* at 5-6 and n. 42. Non-public information on an individual's financial status, employment background, credit history, and medical records can be found in a credit report, but the dissemination of that information by a credit reporting agency is strictly regulated under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1997).

18. *Id.* at 25-28.

19. *Id.* at 28-30.

20. *Id.* at 31-32.

21. *Id.* at 32-33.

22. See *FTC v. Maher*, Case No. WMN-98-495 (D. Md. filed Feb. 19, 1998) (unsolicited commercial e-mail promoting allegedly bogus business opportunity); *FTC v. Cooley*, CIV-98-0373-PHX-RGS (D. Ariz. filed Mar. 4, 1998) (unsolicited commercial e-mail promoting allegedly fraudulent credit repair services).

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

24. FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996.

25. See Transcript from FTC Public Workshop on Consumer Information Privacy, June 11, 1997 at 108-112.

26. As noted on page 17 *infra*, the Commission has recently requested information practice guidelines and principles from trade associations and industry groups to determine the current status of these efforts.

27. See Transcript from FTC Public Workshop on Consumer Information Privacy, June 13, 1997 at 81-82.

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

29. *Id.*

30. See Transcript from FTC Public Workshop on Consumer Information Privacy, June 12, 1997, at 156 (citing Westin Survey at 74).

31. *Id.* at 230.

32. *Id.* at 192-93.

33. *Id.*

34. *Id.* at 132-78 (June 13, 1997).

35. *Id.* at 25-26.

36. In response to a petition from the Center for Media Education concerning the information collection practices of "KidsCom," a web site directed to children, the Commission staff issued an opinion letter addressing potential Section 5 violations involved in the collection of personally-identifiable information directly from young children. Letter from Bureau Director Jodie Bernstein to Center for Media Education, July 15, 1997.

37. Letter from Bureau of Competition Assistant Director to Counsel for the DMA, Sept. 9, 1997.

## ELECTRONIC PRIVACY INFORMATION CENTER

# EPIC Online Guide to 105th Congress Privacy and Cyber-Liberties Bills

[http://www.epic.org/privacy/bill\\_track.html](http://www.epic.org/privacy/bill_track.html)

Last Updated July 10, 1997

---

## House of Representatives

**HR 49. Postal Privacy Act of 1997.** To amend title 39, United States Code, to prevent the United States Postal Service from disclosing the names or addresses of any postal patrons or other persons. Introduced by Condit (D-CA) on 1/7/97. Condit statement. Referred to the Committee on Government Reform and Oversight. Referred to the Subcommittee on Postal Service.

**HR 52. Fair Health Information Practices Act of 1997.** A bill to establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes. Introduced by Rep. Condit (D-CA) on 1/7/97. Condit statement. Referred to the Committee on Commerce, and in addition to the Committees on Government Reform and Oversight, and the Judiciary. Referred to the Subcommittee on Human Resources. Referred to the Subcommittee on Health and the Environment. Referred to the Subcommittee on Crime.

**HR 98. Consumer Internet Privacy Protection Act of 1997.** Requires prior written consent before a computer service can disclose a subscribers' personal information to a third party and allows consumers to access and correct information. Introduced by Vento (D-MN) on 1/7/97. Vento statement. Referred to the Committee on Commerce. Referred to the Subcommittee on Telecommunications, Trade and Consumer Protection.

**HR 102.** A bill to require the national instant criminal background check system to be established and used in connection with firearms transfers by November 28, 1997. Introduced by Rep. Barr (R-GE) on 1/7/97. Referred to the Committee on the Judiciary.

**HR 224. Integrity in Voter Registration Act of 1997.** To amend the National Voter Registration Act of 1993 to require each individual registering to vote in elections for Federal office to provide the individual's Social Security number. Introduced by McCollum (R-FL) on 1/7/97. Referred to the Committee on House Oversight.

**HR 231. A bill to improve the integrity of the Social Security card and to provide for criminal penalties for fraud and related activity involving work authorization documents for purposes of the Immigration and Nationality Act.** Requires creation of tamperproof Social Security card. Introduced by McCollum (R-FL) on 1/1/97. McCollum statement. Referred to the Committee on the Judiciary, and in addition to the Committee on Ways and Means. Referred to the Subcommittee on Immigration and Claims. Subcommittee hearings held on 5/13/97. Referred to the Subcommittee on Social Security.

**HR 273. Food Stamp Fraud Act of 1997.** Expands use of electronic funds transfers with

build in capability for "law enforcement monitoring." Required extensive electronic records of purchases to be kept. Expands access to financial records. Introduced by Schumer (D-NY) on 1/7/97. Referred to the Committee on Agriculture. Referred to the Subcommittee on Department Operations, Nutrition and Foreign Agriculture.

**HR 275. Effective Antiterrorism Tools for Law Enforcement Act of 1997.** Expands use of illegal wiretapping evidence in court, roving taps, pen registers, and collection of travel information. Introduced by Schumer (D-NY) and Conyers (D-MI) on January 7, 1997. Referred to the Committee on the Judiciary. Referred to the Subcommittee on Crime.

**HR 306. Genetic Information Nondiscrimination in Health Insurance Act of 1997.** A bill to prohibit discrimination against individuals and their family members on the basis of genetic information, or a request for genetic services. Introduced by Slaughter (D-NY). Slaughter statement. Referred to the Committee on Commerce, and in addition to the Committees on Ways and Means, and Education and the Workforce. Referred to the Subcommittee on Health and the Environment. Referred to the Subcommittee on Health. Referred to the Subcommittee on Employer-Employee Relations.

**HR 341. Genetic Privacy and Nondiscrimination Act of 1997.** A bill to establish limitations with respect to the disclosure and use of genetic information. Introduced by Stearnes (R-FL) on 1/7/97. Referred to the Committee on Commerce, and in addition to the Committees on Government Reform and Oversight, and Education and the Workforce. Referred to the Subcommittee on Health and the Environment. Referred to the Subcommittee on Human Resources. Referred to the Subcommittee on Employer-Employee Relations.

**HR 470. Eliminate the Magnet for Illegal Immigration Act of 1997.** Limits number of documents that can be used for employment verification. Introduced by Filner on 1/21/97. Referred to the Committee on the Judiciary, and in addition to the Committee on Education and the Workforce. Referred to the Subcommittee on Immigration and Claims.

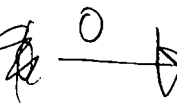
**HR 503. To amend the General Education Provisions Act to allow State and county prosecutors access to student records in certain cases.** . Allows prosecutors to access student records without a warrant in any criminal investigation or prosecution of a student. Introduced by Andrews (D-NJ) on 2/4/97. Referred to the Committee on Education and the Workforce. Referred to the Subcommittee on Children, Youth and Families.

**HR 537. Background Security Records Act of 1997.** Amends Presidential Records Act of 1978 and the Privacy Act, to ensure that Federal Bureau of Investigation records containing sensitive background security information that are provided to the White House are properly protected for privacy and security. Introduced by Maloney (D-NY) on 2/4/97. Referred to the House Committee on Government Reform and Oversight. Referred to the Subcommittee on National Security, International Affairs, and Criminal Justice.

**HR 695. Security and Freedom Through Encryption (SAFE) Act.** Relaxes export controls on cryptography, prohibits mandatory key escrow. Creates new criminal penalties for using encryption to further a criminal act. Introduced by Goodlatte (R-VA) on 2/12/97 w/ 70 co-sponsors. Referred to the Committee on the Judiciary, and in addition to the Committee on International Relations. Hearings held by Subcommittee on Courts and Intellectual Property on 3/20/97. EPIC Testimony. Referred to the Subcommittee on International Economic Policy and Trade. Subcommittee mark-up and forwarded to full Committee by voice vote on 5/14/97. Committee consideration and mark-up held on 5/14/97. Ordered reported (amended) by voice vote on 5/14/97.

**HR 753. Intelligence Budget Accountability Act of 1997.** Requires publication of total intelligence budget. Introduced by Conyers (D-MI) on 2/13/97. Referred to the Committee on the Budget, and in addition to the Committee on Intelligence.

**HR 774. Internet Freedom and Child Protection Act of 1997.** Requires internet service providers to offer filtering software. Introduced by Lofgren (D-CA) on 2/13/97. Referred to the Committee on Commerce. Referred to the Subcommittee on Telecommunications, Trade and Consumer Protection.

 **HR 1180. Family-Friendly Internet Access Act of 1997.** Requires internet service providers to offer filtering software. Introduced by McDade (R-PA) on 3/20/97. Referred to the Committee on Commerce. Referred to the Subcommittee on Telecommunications, Trade and Consumer Protection.

 **HR 1226. Taxpayer Browsing Protection Act.** Criminalizes "browsing" of taxpayer files by IRS employees. Introduced by Archer (R-TX) on 4/8/97. Passed by the House April 15, 1997. Placed on the Calendar in the Senate (CR S3346) on 4/17/97. See the [EPIC IRS Privacy Page](#).

**HR 1227. Internal Revenue Service Accountability Act.** Criminalizes "browsing" of taxpayer files by IRS employees. Introduced by Dunn (R-WA) on 4/8/97. See HR 1226.

**HR 1271. FAA Research, Engineering, and Development Authorization Act of 1997.** Funds FAA projects for new surveillance technologies such as advanced X-ray systems for individuals. Introduced on 4/10/97 by Morella (R-Md). Referred to the House Committee on Science. Approved by Committee 4/16/97. Reported to the House H. Rept. 105-61 (CR H1714) on 4/21/97. Measure adopted on 4/29/97, RC #95 (414-7), (CR H1995). Referred to Senate Committee on Commerce, Science and Transportation (CR S3843) on 4/30/97.

**HR 1287. Social Security On-line Privacy Protection Act of 1996.** Prohibits computer service (such as Lexis-Nexis) from disclosing person's SSN without permission. Introduced by Franks (R-NJ) on 4/10/97. Referred to the Committee on Commerce. Referred to the Subcommittee on Telecommunications, Trade and Consumer Protection. See the [EPIC SSN Page](#)

**HR 1330. American Family Privacy Act of 1997.** Prohibits Federal officers and employees from providing access to social security account statement information, personal earnings and benefits estimate statement information, or tax return information of an individual through the Internet or without the written consent of the individual, and to establish a commission to investigate the protection and privacy afforded to certain Government records. Introduced by Kanjorski (D-PA) on 4/15/97. Referred to the Committee on Government Reform and Oversight. Congressman Kanjorski's [statement](#). Referred to the Subcommittee on Government Management, Information and Technology. See the [EPIC SSA Privacy Page](#)

**HR 1331. Social Security Information Safeguards Act of 1997.** Requires the Commissioner of Social Security to assemble a panel of experts to assist the Commissioner in developing appropriate mechanisms and safeguards to ensure confidentiality and integrity of personal Social Security records made accessible to the public. Introduced by Kennelly (D-CT) on 4/15/97. Referred to the Committee on Ways and Means. See the [EPIC SSA Privacy Page](#)

**HR 1367. Federal Internet Privacy Protection Act of 1997.** Prohibits Federal agencies from making available through the Internet certain confidential records with respect to individuals, and to provide for remedies in cases in which such records are made available through the Internet. Introduced by Barrett (D-WI) on 4/17/97. Referred to the Committee on Government Reform and Oversight. Referred to the Subcommittee on Government Management, Information and Technology. See the [EPIC SSA Privacy Page](#)

**H.R.1428 Voter Eligibility Verification Act.** Establishes a system through which the Commissioner of Social Security and the Attorney General respond to inquiries made by election officials concerning the citizenship of voting registration applicants and to amend

the Social Security Act to permit States to require individuals registering to vote in elections to provide the individual's Social Security number. Introduced by Horn (R-CA) on 4/24/97. Referred to the Committee on the Judiciary, and in addition to the Committees on House Oversight, and Ways and Means. Referred to the Subcommittee on Immigration and Claims.

**H.R.1440, A bill to require the Department of Education to provide links to databases of information concerning scholarships and fellowships.** Introduced by Engel (D-NY) on 4/24/97. Referred to the House Committee on Education and the Workforce. Referred to the Subcommittee on Postsecondary Education, Training and Life-Long Learning.

**H.R.1471, Auto Theft Deterrent Act of 1997.** Directs the Secretary of Transportation to determine the feasibility of placing bar codes on passenger motor vehicles to facilitate the tracing of stolen vehicles. Introduced by Ackerman (D-NY) on 4/29/97. Referred to the House Committee on Commerce. Referred to the Subcommittee on Telecommunications, Trade, and Consumer Protection.

**H.R.1546, Government Secrecy Act of 1997.** Provides for a system to classify information in the interests of national security and a system to declassify such information. Introduced by Hamilton (D-IN) on 5/7/97. Referred to the Committee on Government Reform and Oversight, and in addition to the Committees on Intelligence (Permanent Select), and National Security.

**H.R.1775. Intelligence Authorization Act for Fiscal Year 1998.** Authorizes appropriations for fiscal year 1998 for intelligence and intelligence-related activities of the US Government. Introduced by Goss (R - FL) on 6/4/97. Referred to the House Select Committee on Intelligence. Committee consideration and mark-up session held on 6/5/97. Reported to the House from the Select Committee on Intelligence with amendment (H. Rept. 105-135, Part I), (CR H3923), on 6/18/97. Referred sequentially to the House Committee on National Security (CR H3923) for consideration for a period ending not later than 7/1/97.

**H.R.1813. Personal Information Privacy Act of 1997.** Protects the privacy of the individual with respect to the social security number and other personal information. Introduced by Kleczka (D - WI) on 6/5/97. Referred to the Committee on Ways and Means, and in addition to the Committees on Banking and Financial Services, and the Judiciary. Referred to the Subcommittee on Financial Institutions and Consumer Credit.

**H.R.1815. Medical Privacy in the Age of New Technologies Act of 1997.** Protects the privacy of health information in the age of genetic and other new technologies. Introduced by McDermott (D - WA) on 6/5/97. Referred to the Committee on Commerce, and in addition to the Committee on Government Reform and Oversight.

**H.R.1964. Communications Privacy and Consumer Empowerment Act.** The bill requires the Federal Trade Commission and FCC to conduct reviews of privacy and to propose changes in regulations, promotes screening software for blocking content, orders NTIA to conduct survey on network security and reliability, prohibits restriction of crypto sales in interstate commerce and the requirement of key escrow by federal or state officials. Introduced by Markey (D - MA) on 6/19/97. Referred to the House Committee on Commerce.

**H.R. 1972. Children's Privacy Protection and Parental Empowerment Act of 1997.** Introduced by Rep. Bob Franks (R-NJ) on June 19, 1997. Prohibits "list brokers" from selling, purchasing info about children without written consent of parent. Requires marketers to give access about child to parent, prohibits using prison inmate labor to process childrens' info. Requires marketers to give lists to National for Missing and Exploited Children for data matching purposes. The bill has 30 cosponsors.

**H.R.2063, A bill to direct the Secretary of Health and Human Services to make available to the Secretary of the Treasury information from the National Directory of New Hires for use in collecting delinquent debt owed to the Federal Government.**

Introduced by Maloney (D - NY) on 6/25/97. Referred to the House Committee on Government Reform and Oversight.

---

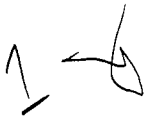
## Senate

**S. 3. Omnibus Crime Control Act.** Eliminates exclusionary rule for illegal searches including illegal wiretaps. Expands penalties for cellular phone interceptions. Introduced by Hatch (R-UT) on 1/22/97. Hatch statement. Referred to the Committee on the Judiciary.

**S. 24. Health Care Assurance Act of 1997.** Creates "centrally located" national database of health insurance information for processing all claims and outcomes. Gives grants to states to create and operate health care cost containment and quality information systems that contain clinical and treatment data on patients. Introduced by Specter (R-PA) on 1/21/97. Referred to the Committee on Finance.

**S. 89. Genetic Information Nondiscrimination in Health Insurance Act of 1997.** Prohibits denial of insurance based on genetic information. Prohibits insurance companies from requesting genetic information. Prohibits disclosing genetic information without written consent. Introduced by Snowe (R-ME). Referred to the Committee on Labor and Human Resources.

**S. 103. United States Worker Protection and Illegal Immigrant Deterrence Act of 1997.** Requires President to recommend creation of national workplace verification system within 90 days. Introduced by Kennedy (D-MA) on 1/21/97. Referred to the Committee on the Judiciary.

 **S. 144. Commission to Study the Federal Statistical System Act of 1997.** Creates Commission to look at statistical agencies. Commission will look at privacy implications of collection and use of statistical information. Introduced by Moynihan (D-NY) on 1/21/97. Referred to the Committee on Governmental Affairs.

**S. 213. Bill to amend section 223 of the Communications Act of 1934 to repeal amendments on obscene and harassing use of telecommunications facilities made by the Communications Decency Act of 1996.** Repeals part of Communications Decency Act and replaces it with original provision on telephone harassment. Introduced by Leahy (D-VT) on 1/28/97. Leahy statement. Feingold statement. Referred to the Committee on Commerce, Science, and Transportation.

**S. 255. Law Enforcement and Public Safety Telecommunications Empowerment Act.** Allocates 24 MHz of spectrum for law enforcement and public safety use. Introduced by McCain on 2/4/97. Referred to the Committee on Commerce, Science, and Transportation. statement.

**S. 376. Encrypted Communications Privacy Act of 1997.** Relaxes export controls on cryptography. Encourages key escrow infrastructure. Creates new criminal penalties for using encryption to further a criminal act. Introduced by Leahy (D-VT) on 2/27/97. Referred to the Committee on Judiciary.

**S. 377. Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997.** Relaxes export controls on cryptography. Creates secret Information Security Board that would give law enforcement agencies special access to the development of new plans for privacy enhancing technologies. Introduced by Burns (R-MT) on 2/27/97. Referred to the

Committee on Commerce. Hearings held 3/19/97.

**S. 422. Genetic Confidentiality and Nondiscrimination Act of 1997.** Defines the circumstances under which DNA samples may be collected, stored, and analyzed, and genetic information may be collected, stored, analyzed, and disclosed, to define the rights of individuals and persons with respect to genetic information, to define the responsibilities of persons with respect to genetic information, to protect individuals and families from genetic discrimination, to establish uniform rules that protect individual genetic privacy, and to establish effective mechanisms to enforce the rights. Introduced by Domenici (R-NM) on 3/11/97. Referred to the Committee on Labor and Human Resources.

26  
**S. 504. Children's Privacy Protection and Parental Empowerment Act of 1997.**

Prohibits the sale of personal information about children without their parents' consent. Introduced by Feinstein (D-CA) on 3/20/97. Referred to the Committee on the Judiciary. See EPIC Kids Privacy Page.

**S. 512. Identity Theft and Assumption Deterrence Act of 1997.** Criminalizes identity theft. Requires FTC to conduct study. Introduced by Kyl (R-AZ) on 3/21/97. Referred to the Committee on the Judiciary.

**S. 521. Taxpayer Privacy Protection Act.** Criminalizes "browsing" of tax records by IRS employees. Introduced by Coverdell (R-GA) on 4/8/97. See S. 522.

**S. 522. Taxpayer Browsing Protection Act.** Criminalizes "browsing" of tax records by IRS employees. Introduced by Coverdell (R-GA) on 4/8/97. Passed by the Senate, April 15, 1997. See EPIC IRS Page.

**S. 523. Taxpayer Privacy Protection Act.** Criminalizes "browsing" of tax records by IRS employees. Introduced by Glenn (D-OH) on 4/8/97. See S. 522.

**S. 600. Personal Information Privacy Act of 1997.** Amends FCRA to prohibit sale on non-public information, prohibits use of SSN as ID number, limits use of SSN on drivers licenses. Introduced by Feinstein (D-CA) on 4/16/97. Referred to the Committee on Finance. Feinstein floor statement. See the EPIC SSN Page

15  
**S.665. Telecommunication Act Progress Report Act.** Monitors the progress of the Telecommunications Act of 1996. Introduced by Kerrey (D-NE) on 4/29/97. Referred to the Committee on Commerce, Science, and Transportation.

**S.712. Government Secrecy Act of 1997.** Provides for a system to classify information in the interests of national security and a system to declassify such information. Introduced by Moynihan (D-NY) on 5/7/97. Read twice and referred to the Committee on Governmental Affairs. Hearings held on 5/7/97.

1 ✓  
**S.771. A bill to regulate the transmission of unsolicited commercial electronic mail, and for other purposes.** Introduced by Murkowski (R- AK) on 5/21/97. Read twice and referred to the Committee on Commerce.

**S.805. Department of Agriculture Information Technology Reform Act.** Reforms the information technology systems of the Department of Agriculture. Introduced by Lugar (R - IN) on 5/23/97. Referred to the Committee on Agriculture.

6 ✓  
**S.874. A bill to amend title 31, United States Code, to provide for an exemption to the requirement that all Federal payments be made by electronic funds transfer.**

Introduced by Faircloth (R - NC) on 6/10/97. Referred to the Committee on Finance.

**S.875. Electronic Mailbox Protection Act of 1997.** Promotes online commerce and communications, by protecting consumers and service providers from the misuse of

computer facilities by others sending bulk unsolicited electronic mail over such facilities. Introduced by Torricelli (D - NJ) on 6/11/97. Referred to the Committee on Commerce.

**S.909. Secure Public Networks Act.** Facilitates national key escrow system. Orders networks built with govt money to use key escrow. Codifies existing restrictions on export on encryption software. Introduced by McCain (R - AZ) on 6/16/97. Referred to the Committee on Commerce. Committee ordered bill to be reported favorably with an amendment in the nature of a substitute on 6/19/97. Hearings held before Senate Judiciary Committee 7/9/97.

---

Return to [EPIC Privacy Page](#) | [EPIC Home Page](#).

# PENDING PRIVACY BILLS

| Bill No./ Date                             | Sponsor              | # Co-Sponsors | Description                                                                                                                                                                                                                                                                        |
|--------------------------------------------|----------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H.R. 52: 1/7/97                            | Rep Condit (D-CA)    | 1             | Establishes a code of fair information practices for health information                                                                                                                                                                                                            |
| H.R. 98: 1/7/97                            | Rep Vento (D-MN)     | 12            | Prohibits an interactive computer service from disclosing to a third party any personally identifiable information provided by a subscriber without the subscriber's written consent                                                                                               |
| H.R. 537:<br>2/4/97                        | Rep Maloney (D-NY)   | 0             | Amends Presidential Records Act of 1978 and the Privacy Act to ensure that FBI records containing sensitive information are protected for privacy and security.                                                                                                                    |
| H.R. 695:<br>2/12/97                       | Rep Goodlatte (R-VA) | 165           | Relaxes export control on encryption devices and creates new criminal penalties for using encryption to further a criminal act                                                                                                                                                     |
| H.R. 774:<br>2/13/97                       | Rep. Lofgren (D-CA)  | 27            | Requires internet service providers to offer filtering software; also amends Communications Act of 1934 to repeal provisions prohibiting using telecommunications device to make or initiate transmission of an obscene communication or depiction of sexual activities to a minor |
| H.R. 1180:<br>3/20/97                      | Rep. McDade (R-PA)   | 0             | Requires internet service providers to offer filtering software.                                                                                                                                                                                                                   |
| H.R. 1226:<br>4/15/97 (Sim to S 522 & 523) | Rep Archer (R-TX)    | 27            | Criminalizes "browsing" of taxpayer files by IRS employees; on Senate Calender as of 4/17/97                                                                                                                                                                                       |
| H.R. 1287:<br>4/10/97                      | Rep Franks (R-NJ)    | 10            | Prohibits computer services from disclosing a person's SSN without permission                                                                                                                                                                                                      |

|                       |                          |    |                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H.R. 1330:<br>4/15/97 | Rep Kanjorski<br>(D- PA) | 18 | Prohibits Federal officers and employees from providing access to Soc Sec Acct information, personal earnings and benefits estimate statement information, or tax return info through the Internet or without written consent of the individual, and to establish a commission to investigate the protection and privacy afforded to certain Gov't records |
| H.R 1331:<br>4/15/97  | Rep Kennelly<br>(D-CT)   | 0  | Establishes a panel to assist the Commissioner of Soc Sec in developing appropriate mechanisms and safeguards to ensure confidentiality and integrity of personal SS records made accessible to the public                                                                                                                                                 |
| H.R. 1367:<br>4/17/97 | Rep Barrett, T.          | 9  | Prohibits Fed agencies from making available through the Internet certain confidential records, and providing for remedies in cases in which such records are made available through the Internet                                                                                                                                                          |
| H.R. 1972:<br>6/19/97 | Rep Franks (R-<br>NJ)    | 30 | Prohibits "list brokers" from selling, purchasing info about children without written consent of parent; requires marketers to give access about child to parent, prohibits using prison inmate labor to process childrens' info; requires marketers to give lists to National Center for Missing and Exploited Children                                   |
| S 144: 1/21/97        | Sen Moynihan<br>(D-NY)   | 1  | Creates Commission to look at statistical agencies; it will look at privacy implications of collection and use of statistical information                                                                                                                                                                                                                  |
| S 376: 2/27/97        | Sen Leahy (D-<br>VT)     | 4  | Relaxes export controls on cryptography. Creates new criminal penalties for using encryption to further a criminal act. Encourages key escrow infrastructure.                                                                                                                                                                                              |
| S 377: 2/27/97        | Sen Burns (R-<br>MT)     | 22 | Relaxes export controls on cryptography. Creates Board to give law enforcement agencies special access to development of plans for privacy enhancing technology.                                                                                                                                                                                           |
| S. 504: 3/20/97       | Sen Feinstein<br>(D- CA) | 2  | Prohibits sale of personal information about children without their parents' consent                                                                                                                                                                                                                                                                       |

|                |                        |   |                                                                                                                                                                     |
|----------------|------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S 665: 4/29/97 | Sen Kerrey (D-NE)      | 1 | Monitors the progress of the Telecommunications Act of 1996                                                                                                         |
| S 771: 5/21/97 | Sen Murkowski (R- AK)  | 1 | Regulates the transmission of unsolicited commercial e-mail.                                                                                                        |
| S 875: 6/11/97 | Sen Torricelli (D- NJ) | 0 | Promotes online commerce and communications by regulating transmission of bulk unsolicited e-mail                                                                   |
| S 909: 6/16/97 | Sen McCain (R-AZ)      | 2 | Facilitates national key escrow system; orders networks built with gov't money to use key escrow. Maintains existing restrictions on export on encryption software. |