Individual Reference Services- A Report to Congress
December 1997

Table of Contents

Executive Summary

In the past year, there has been growing public concern about computerized databases that collect and disseminate personal identifying information about consumers. At the request of three United States Senators, the Federal Trade Commission has conducted a study of 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 has gathered information about the individual reference services industry by soliciting public comments and holding a public workshop in June 1997. At the workshop, industry members announced that they had formed the "Individual Reference Services Group," or "IRSG Group" and intended to draft a self-regulatory framework to address concerns associated with their industry. Commission staff has worked with this group to encourage it to adopt an effective self-regulatory proposal.

This report summarizes what the Commission has learned about the individual reference services industry, examines the benefits, risks, and potential controls associated with these services, and assesses the viability of the IRSG Group's proposal. The report concludes with recommendations that address concerns left unresolved by the proposal.

A vast amount of information about consumers is available through individual reference services. This information is gleaned from various public sources, such as public records and the telephone directory, and non-public sources, such as "credit header" information from credit bureaus (which typically contains name, aliases, birth date, Social Security number, current and prior addresses, and phone number). Information contained in individual reference services' databases 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.

Convenient access to so much information about individuals through individual reference services confers myriad benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, public interest groups to find missing children, banks and corporations to prevent fraud, journalists to report the news, lawyers to locate witnesses, and consumers to find lost relatives. At the same time, the increasing availability of this information poses various risks of harm to consumers. One harm is to consumers' privacy interests; many consumers are increasingly concerned that personal information is so widely available. Consumers also may be harmed in more concrete ways. For instance, the easy availability of this information could lead to increased incidence of identity theft.

The IRSG Group has developed and agreed to a set of principles that regulates the availability of information obtained from non-public sources through individual reference services by implementing the voluntary restrictions described in this report. Restrictions on access to certain non-public information vary according to the category of customer; customers that have less restricted access to non-public information are subject to greater controls. It is particularly noteworthy that the principles prohibit distribution to the general public 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.

Most importantly, the principles show particular promise because they include a compliance assurance mechanism and are likely to influence virtually the entire individual reference services industry. Members must undergo an annual compliance review by a third- party, the results of which will be made public, and members that are information suppliers are prohibited from selling to entities who fail to comply. Thus, the 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 non-public information about them in the services' databases.

The Commission commends members of the IRSG Group for the commitment and concern they have shown in drafting and agreeing to comply with an innovative and far-reaching self-regulatory program. The principles address most of the concerns associated with the increased availability of non-public information through individual reference services while preserving important benefits conferred by this industry.

Despite the laudable efforts of the IRSG Group, important issues related to individual reference services remain. The IRSG principles do not give consumers access to the public information 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 in eighteen months, and to consider whether to conduct a study quantifying the extent of any such inaccuracies. The Commission strongly urges the IRSG Group to conduct an objective 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.

The Commission also encourages 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. Furthermore, the Commission is concerned that individuals may be adversely affected by errors in information obtained through look-up services; therefore, the Commission encourages businesses that rely on such information in making adverse decisions (where not already required by law) to voluntarily notify affected consumers of the sources of the information, as long as such notification would not impede law enforcement or fraud prevention. Finally, the Commission acknowledges and encourages the ongoing efforts of many privacy advocates, consumer groups, government agencies, and the IRSG Group to educate the public about information privacy issues. The Commission looks forward to working with all of these groups in this important effort.

I. Introduction

Computerized database services that sell personal identifying information about consumers -- often referred to as "individual reference services," "look-up services," or "locators" -- drew considerable public and media attention in the fall of 1996. At issue was the perceived sensitivity of the information these computerized database services gather about consumers without their knowledge or consent (*e.g.*, Social Security numbers) and the ease with which such information can be accessed.(1) In October of 1996, three United States Senators reacted to these concerns by requesting that the Federal Trade Commission (the "Commission" or "FTC") conduct a study of these computerized database services (hereinafter "individual reference services," "look-up services," or "services").(2)

In March of 1997, the Commission announced it would conduct a study of individual reference services used primarily to identify, locate, or verify the identity of an individual.(3) Services used primarily for direct marketing, for obtaining medical and student records, or for purposes subject to the Fair Credit Reporting Act ("FCRA") fall outside the scope of the study.(4) Subsequent to the Commission's announcement, members of the individual reference services industry informed the Commission that they planned to create a self-regulatory framework to address concerns related to their industry. The Commission has since gathered information about the look-up services by soliciting public comments and conducting a public workshop,(5) and Commission staff has engaged in an ongoing dialog with industry members as they worked to craft an effective self-regulatory framework. This report describes (1) the individual reference service industry before implementation of the self-regulatory guidelines, including the types and sources of information available through these services, and how these services are used; (2) the benefits and risks associated with the availability of this information; and (3) the viability of existing and potential controls, including the industry's proposed self-regulatory framework. It concludes with the Commission's recommendations in response to concerns associated with the individual reference services industry.

II. The Industry

A. The Overview

Personal identifying information -- information that can be used to identify, locate, or verify the identity of an individual(6) -- has been publicly available for some time. Historically, the government, creditors, insurers, and employers have requested or required from individuals information like name, aliases, address, telephone number, date of birth, and Social Security number; individuals in turn have provided such data in return for certain benefits and services. Moreover, law enforcement agents, private investigators, lawyers, and news reporters have accessed this information for decades in their efforts to track down targets, subjects, heirs, witnesses, etc.

What has happened to make the availability of personal identifying information suddenly spark such far-reaching interest and concern? In recent years, advances in computer technology have made it possible for more detailed identifying information to be aggregated and accessed more easily and cheaply than ever before.(7) In other words, much more richly-detailed data is readily accessible to many more people. Not that long ago, for example, a private investigator hired to track down the location of a non-custodial parent who owed child support would have had to drive around town, from courthouses to county records offices and from the public library to the local department of motor vehicles. Standing in one line to access the records and waiting in another to make copies, he likely would have to fill out forms to send away for still more records from agencies not accessible by car or for records in storage. Ultimately, the investigator would have to sit down and analyze the stacks of paper before him, in the hope of distilling, without the benefit of any information from most out-of-state agencies, his target's current address. This scenario would play out much differently today. Now, by keying in a few search terms at his laptop, in the comfort of his office, an investigator who subscribes to a look- up service can probably track down virtually everything he needs to know to have his target personally served with legal documents. The difference between the costly and time-consuming search once required and the easy and inexpensive retrieval of information now possible can be viewed as a difference in kind, not just degree.(8)

This transformation is due in part to several technological developments. First, data is increasingly available in electronic form.(9) Second, it is now easier to combine data from multiple sources and create comprehensive information products.(10) Third, computer processing speeds have increased.(11) Fourth, the cost of data storage has dropped dramatically.(12) Finally, personal computers are becoming more affordable,(13) and Internet use is growing more prevalent.(14)

In part due to these developments, the market for personal information, already a multi- billion dollar industry, is growing larger and more diverse.(15) Long-time members of the information industry as well as newcomers are responding to the swelling demand by launching new and increasingly comprehensive personal identifying information products and marketing them to a broadening spectrum of potential customers.(16) As a result, providers of information used to locate, verify, and identify individuals have emerged as a discrete industry.(17)

B. Types and Sources of Information Available

Individual reference service databases contain information about an overwhelming proportion of the population, including children. For example, one prominent individual reference service recently promoted one of its databases as containing the names, current and former addresses,

Social Security numbers, and telephone numbers of 160 million individuals.(18) The information is gathered from a wide variety of sources. It typically originates from the consumers themselves, who provide identifying information when they, for example, register to vote, apply for a driver's license, have a new telephone connected, order a catalogue, or apply for credit.(19) Individual reference services then gather this information from public records (like real estate records), publicly available sources (like telephone directories), and from non-public sources (like credit reporting agencies). Alternatively, look-up services may obtain the information from "information vendors," entities that gather data from various sources and either resell it or allow customers to access databases maintained by the information vendors themselves (known as "gateway access").(20) The *types* of information gleaned from these various sources overlap a great deal. For example, an individual's mailing address may be reflected in records obtained from public records, from other public sources, and from non-public sources.

1. Information from Public Records

Public records are a rich source of personal identifying information. Government entities at all levels require individuals to provide various types of information and are usually required to make such records available for public inspection.(21) These records include, but certainly are not limited to, real property records, marriage and divorce records, birth certificates, driving records, driver's licenses, vehicle titles and registrations, civil and criminal court records, parole records, postal service change-of-address records, voter registration records, bankruptcy and lien records, incorporation records, workers' compensation claims, political contributions records, firearms permits, occupational and recreational licenses, filings pursuant to the Uniform Commercial Code (UCC), and filings with the Securities and Exchange Commission (SEC).(22)

Public records may contain extensive and detailed information (*e.g.*, race, gender, Social Security number, address, and dates of birth, marriage, and divorce).(23) Land records, for example, typically include property address and description, dates of sales, sales prices, size of mortgage amounts, and sellers' and purchasers' names.(24) Social Security numbers are available from the records kept by dozens of government entities, such as motor vehicle bureaus and the SEC. Dates of marriage and divorce may be gleaned from marriage and divorce certificates, respectively. Dates of birth may be available from birth certificates and voter registration records.(25) Professional license records may include name, address, type of license held, and in some cases, the date of the license-holder's last medical examination.(26) Driver's license records(27) make available in one place an individual's name, address, height, weight, gender, eye color, date of birth and, in some cases, Social Security number.(28)

Certain agencies, like the SEC, make records available gratis,(29) but in general government records must be purchased for a nominal fee.(30) For example, the State of New York sells driver's license information in the form of abstracts for approximately five dollars each.(31) These abstracts can include such data as vehicle and ownership information, driver's license records, accident reports, conviction certificates, police reports, complaints, satisfied judgment records, hearing records, and closed suspension revocation orders.(32)

Although government records are increasingly available in electronic form,(33) many still must be transcribed. Individual reference services obtain public records information either directly from the government custodian of records, or indirectly, through information vendors who transcribe it (if necessary) and resell it.(34)

2. Information from Other Public Sources

Publicly available information is another fertile source for personal identifying information. Articles and classified ads in newspapers, magazines, and other publications often provide identifying and background information on individuals.(35) Powerful search engines, now available both through the Internet and proprietary networks, enable people to comb through vast amounts of published materials and find all references to a given individual.(36) White pages directories, whether in paper or electronic form, are a readily accessible source of identifying information. The Internet and CD-ROMs now make it possible to find names, phone numbers, and addresses for people all over the country using one database. Other types of more specialized directories have become prevalent as organizations like alumni groups and professional organizations publish their membership directories on the World Wide Web (the "Web").(37) In fact, many new Web sites may prove to be abundant storehouses of information. Such Web sites include not just personal home pages, where individuals publish their own identifying information as well their hobbies and interests, but also, for example, adoption pages, where separated children and birth parents post their identifying information in the hope of being found.(38)

3. Information from Non-Public Sources

A third general category of information that can be found in these databases is proprietary, or non-public, information, which the individual reference services must purchase. Non-public information includes survey data, data reported by consumers themselves,(39) identifying data contained in "credit headers," as well as marketing and other data.

A "credit header" is the portion of a credit report that typically contains an individual's name, aliases, birth date, Social Security number, current and prior addresses, and telephone number. The three national credit agencies -- Trans Union, Equifax Credit Information Services (hereinafter "Equifax"), and Experian -- maintain and update this information, which they obtain from creditors, courthouses, and the consumers themselves.(40) Trans Union and Experian currently sell credit header information directly to individual reference services or to information vendors who, in turn, sell it to the services.(41) Information in a credit report other than the "credit header" may reflect an individual's financial status, employment background, credit history, or medical records. The dissemination of this type of information is strictly regulated by the Fair Credit Reporting Act.(42)

Another possible proprietary or non-public source of identifying information for look-up services is marketing information. According to the Direct Marketing Association ("DMA"), which represents more than 3,000 United States corporations, information gathered for marketing purposes, *e.g.*, information gleaned from magazine subscription lists and warranty cards, should not be an information source for individual reference services.(43) The Commission, however, has learned of individual reference services that now offer, or offered until recently, data purportedly originating from marketing transactions.(44)

There are many other potential sources of non-public information. For example, some look-up services claim to obtain information from sources such as phone records, public utility records, and air travel records (indicating the airline, flight number, date, time, and even seat assignment for an individual's departure and return flight).(45) Other look-up services may obtain information elsewhere; however, because not all services reveal their sources for proprietary reasons, it is not possible to provide an exhaustive list.

C. Characteristics of Information Products

Individual reference services sell identifying information as raw data, in the form in which they received it, or they combine data from various sources and create enhanced information products or reports.(46) Accordingly, customers, upon entering search terms, can access information from one or more databases maintained by an individual reference service, or obtain gateway access into a database maintained by another entity.(47) The search may yield a compilation of identifying data used, for example, to locate an individual, or it may compare data entered by the customer to data in the database to verify an individual's identity.(48)

The scope of information offered by individual reference services varies significantly. Virtually all of these services include in their databases individuals' names and aliases, and current and prior addresses. Other services also make available certain unique identifiers, such as Social Security number, date of birth, and mother's maiden name.(49) Additional information may also include: place of birth, names and ages of family members and neighbors, schools attended, telephone numbers (listed and unlisted), employment information (past and present), physical characteristics, licenses held, voter registration information, driver's license number, automobile registration, personal identification numbers, association memberships, census information associated with the addresses, and asset ownership. Searches may also yield information about children, to the extent their identifying information is available.(50)

The number of databases employed by individual reference services to provide this information varies significantly as well. On one end of the spectrum, some look-up services provide access to one database and display, for example, only current and prior addresses. On the other end, one service offered over the Internet claims to offer the following product:

This is an amazing, revolutionary search. For one flat fee, this search takes any individual's name, or a company name, or any topic or subject, and runs it through 1,000 separate computer databases, which warehouse a collective 100 billion records. (Not million. Billion) Any and all information is returned that is found of [sic] the subject; length is unlimited. Many of the databases include Equifax, TRW, DBT, Trans Union, ABI, Dun & Bradstreet, IDS, CDB, Information America, DDI, TRW Business, Metromail, national newspaper database, national magazine database, UCCs, national lien and judgment search, national bankruptcy, national federal tax liens, national collection accounts, national mortgage search, national real property and many, many more. This combined search is truly remarkable. On searches conducted to date, the average report length has been 100 pages.(51)

Many information products fall somewhere between these extremes, yielding, for example, the results of searches of a series of public records databases relating to a particular topic, such as professional licenses or liens and judgments.

The cost to conduct a search ranges from roughly $1.50 to over $500.(52)

The cost is a function of which reference service is offering the product (for example, an offline look-up service may charge $85 for a search that is available over the Internet for less than $10) as well as the depth, detail, and accuracy of the information sought.(53) Certain computerized databases offer identifying information to the public for free over the Internet.(54) The free services typically include access to one database containing public records maintained by government agencies or to white-page directories. Government agencies are increasingly making public records databases available for free over the Internet.(55) White-page directory databases are essentially computerized versions of white pages telephone directories and contain names,

addresses, telephone numbers, and often E-mail addresses. Some of these look-up services allow "reverse" searches, enabling the user to enter the phone number or address and retrieve an individual's name.

D. Procedures Used to Restrict Access to Information

Offline commercial individual reference services have typically utilized proprietary networks (not the Internet) to transfer their information products to customers. Under this arrangement, customers may access the information via modem from a personal computer only after providing accurate and verified identifying and credit information,(56) entering into a subscription and payment agreement with the provider, and obtaining the necessary proprietary software.(57) Most individual reference services operating through their own proprietary networks do not offer their services to the public at large; instead they limit access to their services to what they deem to be legitimate businesses for legitimate purposes.(58) Some look-up services require a sign-up fee and monthly fees in addition to the per-search costs.(59) These costs may be high, further restricting the general public's access. Certain entities that sell information products in bulk to individual reference services impose similar access restrictions on their customers.(60)

The procedures used by the individual reference services to evaluate their customers and their contractual arrangements vary.(61) Some look-up services require new customers to complete an application in which the customer sets forth general purposes for accessing the information and agrees to use the information legally.(62) Other services may require a nexus between the user and the data subject.(63) Some services verify all the information in the application; others make sure that the applicant is a known business by conducting on-site visits(64) or by verifying that the phone number provided in the application matches the one listed in the telephone book under the business' name.(65) The level of scrutiny an applicant must undergo may also vary according to the type of information sought: certain look-up services grant access to public records, for example, with less stringent verification procedures,(66) or restrict access altogether to non-public sensitive information, such as Social Security numbers(67) and information about children.(68) In addition, look-up services may remind customers about permissible uses with messages that appear when the customer attempts to run particular searches.(69)

A few services control risks of misuse by monitoring how their customers are using the databases and by maintaining audit trails of who has accessed which information.(70) Finally, look-up services may terminate or deny service for failure to abide by their procedures.(71)

As mentioned above, individual reference services have begun operating over the Internet.(72) Online services differ from offline services (*i.e.*, services that provide information through a proprietary network, but not over the Internet) in that they may be more readily accessible to a broader spectrum of customers. The range of information provided online parallels information provided through proprietary networks, and may be sold for less money.(73) One online service, for example, is reported to offer its subscribers an individual's Social Security number, birth date, and telephone number for just $1.50.(74)

Providing individual reference services over the Internet may pose unique problems with verification and access restrictions. In fact, several offline companies, acknowledging the risks in providing access to customers with whom they do not have an established business relationship, choose not to provide their non-public information services online.(75) Customers may attempt to access the services from computer terminals away from their home or office with Internet

access accounts that shield their identity. Monitoring the uses by, and/or maintaining an audit trail of information accessed by, a user who successfully remains anonymous would probably not be very helpful in preventing or remedying misuse.

Certain online providers do take precautions to restrict access and prevent misuse. Some refuse to serve customers who are accessing their Web site anonymously,(76) and others require customers to enter into a subscription or use agreement,(77) as is the case with their offline counterparts. The majority of online white-page directory services limit the information they make available in the first place by: providing only information that is accessible from telephone companies, suppressing unlisted directory information, permitting consumers to opt out of having their information made publicly available, and not allowing reverse searches.(78) However, the barriers to entry for setting up a service online are remarkably low; by paying a local Internet service provider as little as $19.95 per month and purchasing information from a vendor, anyone can publish a Web site with whatever information she chooses.(79) Thus, it is possible that some companies providing services online may offer information more widely, with fewer restrictions.

III. Beneficial Uses

Individual reference services cater to a wide array of customers, from law enforcement agents and corporations to public interest groups and individual consumers. Users agree that, although the same information may be available from other sources, having access to computerized databases enables them to obtain the information, and therefore conduct searches and investigations, much more quickly.(80) Additionally, some point out that increased accessibility to more information is necessary because people are becoming more mobile and, accordingly, more difficult to find.(81)

A. Public Sector Uses

Individual reference services provide critical assistance to federal, state, and local government agencies to carry out their law enforcement and other missions.(82) Agencies, including the Federal Trade Commission, rely on the databases to detect perpetrators of fraud, to locate and identify suspects and related businesses, and to track down witnesses.(83) Agencies emphasize the importance of having access to all possible identifying information.(84) A subject's prior addresses may point to locations where other law enforcement agencies may have warrants or case information.(85) Knowing the identities of suspects' neighbors is sometimes necessary for their protection.(86) UCC filings, and lien and judgment records can link individuals and companies.(87)

Computerized databases play a particularly useful role in the prosecution of financial crimes. The Financial Crimes Enforcement Network, an arm of the US Department of the Treasury, (hereinafter "FinCEN") relies heavily on computerized databases to prevent and detect money laundering.(88) FinCEN carries out this mission in part by combining information it receives from banks and other financial institutions with government and public information.(89)

It then discloses the information to other law enforcement agencies in the form of intelligence reports.(90) FinCEN also grants law enforcement officials in each state online access to its financial database.(91) Because so many law enforcement agencies rely on FinCEN for analytical support, FinCEN is even able to connect agencies that are investigating the same crime or individual.(92) The National White Collar Crime Center, a non-profit organization funded by the US Justice Department, also subscribes to individual reference services and, like FinCEN, conducts searches on behalf of member agencies with criminal investigative authority related to economic crimes.(93) In addition, the US Secret Service subscribes to approximately thirteen of these databases. The Secret Service uses them to fulfill its mission to investigate counterfeit currency and financial crimes, by locating targets and detecting fraudulent practices, as well as its mission to protect public officials, by locating individuals who pose a threat or who have information regarding potential threats.

B. Private Sector Uses

Individual reference services provide myriad benefits to the private sector as well.(94) The services play important roles for diverse entities, including insurance companies, banks, creditors, retailers, lawyers, private investigators, non-profit agencies, and journalists. Private sector representatives emphasize that many of their purposes for using these services, like fraud prevention and the enforcement of court orders, overlap with those of law enforcement.(95) In light of the increasing case loads and decreasing budgets of many law enforcement agencies, they note that private sector contributions in these areas are critical.(96)

The corporate sector appears to employ the look-up services primarily to detect and investigate potential fraud. The insurance industry, for example, relies on these services to investigate fraudulent claims.(97) Many people who submit fraudulent insurance claims use a fake name or Social Security number; insurance companies can detect these cases by verifying the claimant's personal identifying information through a service.(98) Credit grantors in the retail and other industries use information provided by the look-up services to confirm the identity of credit applicants.(99) They, too, make sure that all of the identifying information provided by the applicant matches the information retrieved through the services, in order to detect and limit potential fraud.(100) Banks have affirmative obligations to report credit card fraud, insider abuse, and money laundering.(101) To fulfill these obligations, they use the look-up services to: verify the validity of identifying information, such as Social Security numbers, provided by new account applicants;(102) implement required "know your customer" policies;(103) and ensure that potential employees have clean records.(104) Many businesses also subscribe to look-up services to conduct due diligence investigations(105) to minimize the risk of financial fraud in business dealings, and to locate business debtors.(106) Private organizations may also use look-up services in connection with fund-raising efforts.

In relying on look-up services to prevent fraud in connection with credit and job applications, the corporate sector may be using information provided by look-up services to make decisions about whether to grant consumers credit or jobs.(107)

The precise information these entities are using to make such decisions remains unclear.(108) To the extent that entities are making credit, insurance, or employment decisions about individuals based on information in consumer reports (*e.g.*, credit history, financial status, and employment background information), their uses would be subject to certain obligations and restrictions set forth in the Fair Credit Reporting Act.(109)

The legal profession, either directly or through third parties like private investigators, relies on individual reference services for many purposes, including locating witnesses;(110) identifying parties and witnesses with a financial stake in the outcome of cases;(111) finding assets to satisfy judgments;(112) conducting due diligence investigations of financial representations;(113) and locating debtors, heirs, and pension fund beneficiaries.(114) In addition, private investigators use look-up services when hired by businesses to prevent or detect insurance fraud, bank fraud, and identity theft.(115) Finally, they use look-up services on behalf of consumers to reunite families; to locate missing or abducted persons; to carry out prenuptial investigations; to stop stalkers; or to track down non-custodial parents who owe child support.(116)

Many public-interest oriented organizations rely on individual reference services for quasi- law enforcement purposes, such as detecting fraud in connection with campaign financing, finding missing children, curbing domestic violence, and enforcing child support orders.(117) Government watchdog groups and others rely on individual reference services to access Federal Election Commission filings to monitor the records of federal campaign contributions.(118) Agencies such as the Center for Missing and Exploited Children track down abducted children and run-away teens by combining data such as name, address, Social Security number, and school enrollment lists obtained from both private and public databases.(119) Other groups use look-up services to prevent child and elder exploitation in the first place, by conducting background checks of potential care providers.(120) Health care organizations use the look-up services to locate organ and bone marrow donors.(121) The services are also instrumental in assisting organizations find non-custodial parents who have neglected to pay court-ordered child support.(122)

The parents can then provide this information to their government child-support agency or use it to initiate their own court action.(123) These organizations also emphasize the need to have access to as much identifying information as possible. For example, one non-profit agency claims a 90 percent success rate in finding parents who owe child support when provided with a Social Security number, compared to a 57 percent success rate without it.(124)

Individual reference services play an important role in journalism as well. Journalists use the services to ensure the accuracy of their stories, for example, by independently verifying the identity of a news subject.(125) The look-up services also enable reporters to enhance their stories with background information on news subjects, like disaster victims and elected officials.(126) Journalists also emphasize the value of having access to as much identifying information as possible.(127)

C. Consumer Uses

Many of the uses outlined above ultimately benefit consumers. Look-up services that serve consumers, not just businesses, enable individuals to find information for any of the uses outlined in this section, without having to hire an intermediary to do it for them. By using these look-up services (typically offered over the Internet), consumers can independently locate an old friend or family member, verify land title in the course of a real estate transaction, or verify the validity of licenses of medical or other professionals.(128) Furthermore, consumers indirectly benefit from this industry in that fraud prevention in the corporate sector helps to keep consumer prices down.(129) Moreover, society as a whole may benefit to the extent that this industry enables the media to more timely and accurately report the news.

IV. Risks

While the individual reference services industry bestows undeniable benefits on society, the wide availability of personal information also poses risks to consumers' psychological, financial, and physical well-being. Consumers may be adversely affected by a perceived privacy invasion, the misuse of accurate information, or the reliance on inaccurate information. A meaningful risk assessment begins with an acknowledgment that because consumers are not the customers of these companies,(130) the companies have little marketplace pressure to respond to consumer interests. Furthermore, because consumers do not have a direct relationship with look- up services, they may remain unaware of possible exposure to risks.(131) Finally, consumers have few means to protect themselves.(132)

A. Impact on Consumers' Privacy Interests

Survey research over the past 20 years demonstrates that increasing numbers of Americans are concerned about how personal information is being used in the Computer Age.(133) A recent poll indicates that a sizeable majority of Americans -- 88 percent -- are concerned particularly about the sale of their Social Security numbers and other personal identifiers.(134)

With increasing attention to privacy by the press, consumers are only now beginning to learn about the individual reference services industry.(135)The outrage many consumers expressed last year in response to learning about the availability of their Social Security numbers through LEXIS-NEXIS' P-Trak service suggests that they would be even more concerned to learn about the wide availability of sensitive information through other services.(136) Once consumers disclose their information to private entities, or once it is transferred from a public records custodian, where data subjects at least have the possibility of seeing and correcting their own records, consumers essentially lose their ability to access information maintained about them.(137) As data subjects have no relationship with companies offering individual reference services, they have few means to determine which organizations store and communicate information about them to others.(138) Furthermore, given this lack of privity, consumers as data subjects do not necessarily derive a direct benefit from the service.(139) Even if consumers were able to determine who was storing and selling information about them, only in rare instances could they access records containing data about them, correct any errors, find out who has accessed their records, or have their records removed from private databases.(140)

Consumers' concerns about the privacy of their personal information are closely related to the sensitivity, both real and perceived, of that information. The perceived sensitivity of information varies with each individual and with the context in which the information is requested or made available.(141) Many people, for example, are completely comfortable listing their home address in the white pages, while others may take precautions not to disclose this information unless absolutely necessary.(142) Furthermore, while individuals may not be concerned with certain pieces of information when standing alone, they may perceive those same pieces of information as sensitive when integrated together,(143) or when used to uncover more potentially sensitive information (such as using name and birth date to obtain Social Security number).(144) Individuals also may change their idea of what is sensitive as they discover that others are accessing their information for business or other purposes inconsistent with the purpose for which it was originally furnished.(145) For example, an individual may be comfortable providing income information when applying for a loan or a parent may willingly disclose a child's age to register the child in school, but would not want this information made publicly available.(146) Furthermore, many consumers feel comfortable with others being able to discover their phone number or address using their name as a search term, but do not feel comfortable when their

phone number or address is used to find out their name through a "reverse search.(147) Moreover, comfort with the availability of information in the physical world may not transfer to comfort with the availability of the same information over the Internet.(148) Finally, the same piece of information (*e.g.*, age) may raise different privacy concerns at different points in a person's life.(149)

Certain unique identifiers, like Social Security number, are more uniformly perceived as sensitive. This perception is reflected in recent survey findings as well as by the public's response to learning that their Social Security numbers were available through LEXIS-NEXIS' P-Trak service.(150)

This sensitivity is understandable given that many entities use Social Security numbers to identify an individual before either granting access to more information, like a bank account balance, or conferring a benefit, like opening a credit card account.(151) Date of birth(152) and mother's maiden name may be considered sensitive for this same reason.(153)

Surveys conducted regarding consumers' opinions about public records information further illustrate that sensitivity is generally a function of both content and context. Although consumers readily provide their information to government agencies for discrete purposes (or when compelled to do so), they do not support the government making all public records readily available. For example, one survey has found that 92 percent of American adults believe it is at least somewhat important that state agencies not be able to sell or release personal data about them without their knowledge or consent.(154) Similarly, another study concluded that 75 percent of American computer users object to the wide availability of public records via the Internet.(155) A third survey asked consumers how they felt about businesses accessing certain public records to prevent insurance fraud.(156) The survey found that 60 percent of Americans support the use of criminal records to combat insurance fraud and 51 percent support the use of motor vehicle records for that purpose.(157) This support wanes, however, for the use of worker's compensation records (40 percent), health claims data (36 percent), medical records (31 percent), or pharmaceutical data (25 percent) to combat insurance fraud.(158)

B. Risks Associated With Inaccurate Data

It is not difficult to imagine how inaccurate information products could bring real harm to consumers. A doctor whose professional license records are mistakenly excluded from a professional licenses database may have a tough time recruiting new patients. An entrepreneur whose records are crossed with those of a convicted white collar criminal with the same name may not find many willing business partners. Similarly, an operator of a day-care center whose identifying information, because of a typographical error, indicates that a previous address is that of a local strip bar may not stay in business very long.(159) The record reflects that, in an effort to prevent fraud, certain entities use information obtained through the look-up services to decide whether to grant an individual a job or credit.(160) If the information offered by the applicant does not match the information obtained through the look-up services, the applicant may be denied credit or employment. Inaccurate information in the look-up services could cause an honest individual to be denied credit or employment wrongfully. Finally, inaccurate information obtained through a look-up service could result in an individual not being found and therefore not receiving an earned benefit (*e.g.*, pension benefits) or suffering harm (*e.g.*, not learning of prior exposure to toxic chemicals).

Given the ease with which information can be gathered, aggregated, and shared, errors could be widely replicated(161) and the harm long-lasting. As described by one industry representative,

the information obtained through individual reference services is unverified data, entered initially by human beings and accordingly subject to human error.(162) While some companies warn their customers of this up-front,(163) others tout the accuracy of their information products. One large supplier of public records information assures its customers that the information it sells is at least 99 percent accurate.(164) An information industry association states that because these databases aggregate information from several sources, the information products tend to be more accurate.(165) Several industry representatives point out that the information must be accurate because the market demands accuracy.(166)

Even at their source, however, records may contain typographical errors, misspellings, or omissions.(167) Furthermore, once records are transferred to secondary information providers, they may not reflect the most current information (depending on the method of data collection or backlog in updating the records at their source).(168)

They may contain errors caused during the creation of public records indices(169) or during the transcription or transmission of the original records. Moreover, due to overlap in identifying information, the results of a search of records compiled from several sources could reflect a mismatch, displaying accurate information about someone, but not necessarily the targeted individual.(170)

Data subjects generally do not have the ability to access the data maintained about them by individual reference services to correct errors.(171) Consumers may in some cases succeed in obtaining a copy of their records only by hiring a professional to buy the relevant information products from look-up services to which the professional subscribes.(172) Alternatively, consumers could buy information products containing their own identifying information directly from look- up services which have less stringent access requirements. Yet, even if consumers determined that information products contained inaccuracies about them, there currently is no mechanism for correcting errors. Moreover, correcting the error in one database may not solve the problem, as misinformation tends to resurface in the same database,(173) or show up later in others.

Although neither workshop participants nor commenters identified concrete evidence of harm linked directly to inaccurate records offered by look-up services, this can be explained by factors other than the absence of such harm. Most consumers have no way of knowing that adverse decisions affecting them are made based on inaccuracies obtained through the look-up services. First, most consumers are unaware of the existence of look-up services. Second, most look-up services do not maintain audit trails of their customers' uses, and, therefore, cannot determine whether an entity who has made a decision affecting a consumer had in fact used a look-up service to access that consumer's files. Finally, except when users make decisions to deny credit, insurance, or employment based on a consumer report (containing, *e.g.*, credit history, financial status, and employment background information) obtained from the look-up services, the users have no obligation to notify the data subject that an adverse decision was based on information obtained through a look-up service.(174)

C. Risks Associated With Unlawful Uses

Increasing access to personal identifying information also poses troubling risks of unlawful uses. Whether initially obtained by an unscrupulous employee, a scam artist able to side-step access restrictions, a computer hacker,(175) or an Internet surfer, personal identifying information in the wrong hands can have severe repercussions.(176)

One risk is that certain users, although they have an apparently legitimate purpose for accessing information through the service, may exploit their access and use the information for illegal purposes, like fraud. Responsible individual reference services do employ security measures to limit wrongful use, for example by having their customers require employees to sign non-disclosure agreements. Yet, reported incidents about employees in other industries who have access to personal identifying information demonstrate that such measures do not always work. Employees sometimes sell information they obtain from their employers' databases, or exploit it themselves. In one highly-publicized incident, a prison inmate (and convicted rapist), who, along with other inmates, was retained by an information vendor as a data processor, had legitimate access to a database containing personal information, and then used the information to compose and send a personalized, threatening letter to an Ohio grandmother.(177) Additionally, a used car salesman was caught using information in a consumer's credit report for illicit purposes.(178) Similarly, according to the Secret Service, perpetrators of fraud are increasingly buying consumer information from corrupt bank employees.(179)

Wrongful access by hackers is another risk. In response, certain companies have implemented firewalls.(180) Computers, however, are notoriously insecure.(181) Hackers can break into even the most impervious databases searching for information.(182) Three German hackers who successfully penetrated the firewall of an Internet service provider siphoned its entire list of 11,000 customers, including detailed credit applications, and threatened to post it on the Internet.(183) A California man downloaded 100,000 credit card numbers by tapping into the Web sites of online retailers.(184) According to the FBI, reports of wrongful access to information stored in computers have increased more than six-fold since 1991.(185) Furthermore, at the end of the third quarter of 1997, the FBI had 392 pending cases of wrongful access, compared to 99 at the end of 1995.(186) Given the demonstrated insecurity of computers, these risks may persist regardless of any regulation.

Commenters and workshop participants are concerned that identity theft and credit card fraud will increase with the growth of the individual reference services industry.(187) The harm caused by identity theft is not merely the financial exposure of victims,(188) banks, and lending institutions. It sometimes takes years of time and frustration for victims to re-establish their own identities, and their harm is difficult to quantify.(189)

Identity thieves have historically used low-tech means to accomplish their crimes such as stealing pre-approved credit applications from mailboxes or obtaining credit card receipts from trash dumpsters.(190)

A recent case brought by the United States Secret Service, however, demonstrates how computer-savvy identity thieves may exploit information available over the Internet. The defendants, a Maryland couple who were arrested last June and who pled guilty in September, admitted not only to stealing the identities of hundreds of individuals, but also to routinely using Internet databases (accessed at a local community college) to select their victims.(191) According to the Delaware detective who investigated the case, the couple sought affluent individuals who lived in the South, where states typically use Social Security numbers as drivers' license identification numbers.(192) The couple obtained official birth certificates, driver's licenses, credit cards, and bank accounts, and ran up debt exceeding $100,000 under their assumed identities.(193) It is unclear, however, whether they relied on look-up services, or simply gathered information from published materials generally available on the Internet.(194)

Individual reference services potentially could facilitate identity theft and credit card fraud in several ways. First, if the perpetrator has already identified the victim, she could use those

services that display Social Security numbers to obtain the victim's Social Security number and other necessary identifying information. As the Court of Appeals for the Fourth Circuit has observed, "[s]uccinctly stated, the harm that can be inflicted from the disclosure of a Social Security Number to an unscrupulous individual is alarming and potentially financially ruinous.(195) Many services that do not display Social Security numbers do allow searches by Social Security number, so that when a user enters a Social Security number, the service retrieves the record of the individual associated with that number, including name, address, and date of birth.(196) Anyone willing to spend some time and money, therefore, could run searches with strings of nine digits (fabricated Social Security numbers) until she finds an identity worth impersonating.(197) Once an identity thief has selected the name and Social Security number of a potential victim, gaining access to an individual reference service would afford her additional lucrative information, such as the assets and professional licenses associated with that identity. This information would enable the identity thief to select identities with potentially high credit limits.

Industry representatives emphasize that the Federal Reserve Board (hereinafter "FRB") found little hard evidence linking identity theft to the look-up services.(198) However, the FRB concluded that "fraud related to identity theft appears to be a growing risk for consumers and financial institutions, and the relatively easy access to personal information may expand the risk.(199) As discussed above, the lack of concrete evidence may be due to the fact that look-up services often do not keep records of who has accessed which information products. Therefore, it would be difficult, if not impossible, to link a case of identity theft to an individual reference service, unless perpetrators admit to their source for information. It is difficult to know whether the lack of audit trails is preventing the development of evidence linking the look-up services to identity theft. On the other hand, evidence does indicate that databases can be used to *reduce* the risk of identity theft and credit card fraud, because access to credit header information and other verification tools enables database users to detect attempts at wrongful use of Social Security numbers.(200)

Physical harm perpetrated by violent stalkers and domestic abusers is an additional troubling risk associated with look-up services.(201) Regardless of their efforts to conceal their whereabouts, potential victims who provide their new address to credit grantors -- who in turn report it to the credit reporting bureaus, who in turn sell it to the individual reference services -- can be easily found.(202) According to one law enforcement organization, accessing government records is the most common way that rapists locate their victims,(203) and perpetrators of domestic violence can easily find relatives who have relocated in an effort to escape.(204)

Individual reference services make government records easy to access. This fact is particularly unnerving, given that many of these services provide location information about children.(205) The infamous murder of actress Rebecca Schaeffer, whose predator tracked her down by having a private investigator access her DMV records from a computerized database, demonstrates the potential harm.(206) Additionally, many individuals, because of their occupations, are vulnerable to unwanted intrusions at home. Such individuals include: police officers and other employees in the law enforcement and justice systems; teachers; doctors and other health professionals; psychological counselors; social workers; and employees of "unpopular" government agencies.(207) In fact, access to public records information has enabled criminals to track down the residences of their arresting officers.(208) Although the availability of public records information from government custodians already poses risks, the look-up services greatly facilitate access to the public records, and thereby substantially increase those risks.

V. Controls

The commenters and workshop participants recommended various controls that might address the concerns raised by the existence of the look-up services. These controls include: (1) limiting the availability of sensitive identifying information; (2) monitoring how customers use information and maintaining audit trails; (3) allowing consumers to access information maintained about them and to dispute inaccuracies; (4) providing consumers with control over how information about them is used; and (5) educating consumers about the industry, its information practices, and related privacy issues, and educating business about consumer privacy interests. As discussed above, certain members of the industry have implemented some of these controls, and others have not.

A. Limiting the Availability of Sensitive Information

1. Limiting Access to Information Obtained Through Individual Reference Services

Several participants at the June 10, 1997 Workshop and commenters (responding to the Commission's *Federal Register* notice) urge that individual reference services take precautions to limit access to personal identifying information and to prevent its misuse.(209) A core element of fair information practices identified through government efforts is that parties who create, maintain, or disseminate personal identifying information must prevent its misuse by others.(210) Completely barring the availability of all information could eliminate potential benefits, while making information available to everyone without restriction could maximize the potential risks. Accordingly, one approach is to limit access to customers who can be trusted to use it for specified purposes. Given that certain categories of information,(211) and certain types of users, pose more of a threat to consumers, access limitations could be a function of both the category of information sought and the type of user.

Who should have access to what types of information? One potential means to limit access to sensitive information, like Social Security number and birth date, would be to determine on a case-by-case basis whether a particular user has a legitimate purpose to obtain such information.(212) One Workshop participant advocated that such restrictions require that look-up services, before granting access, verify that the user is who she says she is, and that she is a legitimate entity with a legitimate purpose.(213)

Other approaches were also posited. Allowing only law enforcement officials to access information through individual reference services is one alternative approach. However, such a limitation would eliminate not only private sector benefits not directly connected to law enforcement, but perhaps even benefits connected to law enforcement as well. For example, government child support enforcement, and other law enforcement, agencies are burdened with an extreme backlog of cases and often cannot pursue all worthy cases. As a result, several private agencies assert that they help public agencies carry out their law enforcement missions.(214)

Another possibility would be to allow access for only law enforcement-related purposes, and allow the look-up services to be used by public and private agencies for child support enforcement, finding missing children, and other similar ends. Private entities are concerned about this approach, as well. First, it would exclude journalistic uses(215) and important industry uses, like fraud prevention.(216) Second, one panelist suggested that her child support enforcement agency and other public interest groups enjoy free or discounted services.(217) As the services would not be able to make the same profits if they restricted the access of users who would otherwise pay the full cost, the participant was concerned that such restrictions could so

severely impair the companies' profit incentives that they would no longer provide the services,(218) or no longer provide free or discounted services. Yet another suggested approach would be to limit access to regulated or licensed entities, such as lawyers and private investigators, in addition to law enforcement agents.(219) Misuse of information by these parties would have repercussions, such as license revocation.(220) However, not all users who have potentially beneficial purposes for accessing information are regulated entities. This approach would exclude access by private investigators in several states without licensing requirements, journalists, and much of private industry.

2. Minimizing Extraneous Sensitive Identifying Information in Public Records

The increasing availability of public records facilitates easy access to sensitive identifying information which, as described above, could have harmful consequences. Another possible control, therefore, would be to minimize the sensitive identifying information that government entities gather and/or make publicly available.(221)

In general, access to public records furthers important societal objectives. For example, wide dissemination of title information in land registers advances the public notification purposes of land recording statutes.(222) Court records can inform the public about questionable prosecutorial policies, low conviction rates, and fraudulent schemes requiring legislative attention.(223) The availability of professional license information enables consumers to avoid being harmed by the services of unqualified professionals.(224) It is possible, however, that the collection and/or dissemination of sensitive information, like Social Security number, mother's maiden name, and date of birth, does not directly advance the purpose underlying the requirement of a given public record.(225) Limiting the availability of public records once information has been collected by government agencies may raise some concerns; *e.g.*, it could erode the public's right to know,(226) and impose costs on public records custodians.(227) However, continuing to make available information that advances a government agency's intended purpose while minimizing the extraneous, sensitive information could help reduce potential harm.

3. Heightening Security Measures

Commenters expressed concern about protecting the information from *unauthorized* access.(228) Accordingly, they recommended that services minimize risks by heightening security controls. Commenters urged individual reference services to employ technological protections, such as firewalls and encryption, as well as measures to prevent unauthorized disclosures by employees.(229)

B. Monitoring Use and Maintaining Audit Trails

Two additional controls related to access restrictions include monitoring use and maintaining audit trails. Access restrictions based on purpose are meaningful only if controls are in place to ensure that users who obtain information for a stated legitimate purpose actually use information consistently with that purpose.(230) Monitoring the use of information would accomplish this end. Similarly, the maintenance of audit trails -- records of which users have accessed what information -- may enable a company to link misuse to a particular user, and thereby identify instances where users asserted a legitimate purpose but used information wrongfully.(231) Without audit trails indicating to whom and for what purpose information has been sold, some maintain that consumers have no recourse upon being harmed by misuse of their information.(232) Audit trails also may be important at the front end, as a deterrent: if

potential abusers of information knew that the information they obtain could be traced back to them, they arguably would be less likely to misuse it.

Although certain look-up services do maintain audit trails, according to industry members, they are problematic for two reasons: (1) maintaining records of every search run by every customer would be unreasonably costly and (2) because records of what information an attorney accessed could be discoverable in a lawsuit, companies that maintain audit trails might lose attorney clients. Furthermore, audit trails are not completely effective in tracking misuse of information because a wronged consumer or law enforcement entity investigating misuse would first have to know which look-up services were accessed in order to determine which service's audit trails to examine.(233) However, if an entity did know which look-up services were accessed, or if the entity simply inquired with several of the look-up services, audit trails would increase the likelihood that a wrongdoer would be tracked down.

C. Allowing Consumers to Access Their Own Information and Dispute Inaccuracies

Many argue that, at a minimum, consumers must have reasonable access to information maintained about them by individual reference services.(234) Without access to their own records, consumers have no way to know whether information that is disseminated about them is accurate. Consumer access requirements have also surfaced as an integral element of fair information practices in several similar contexts.(235)

For example, consumer access has proven to be critical in the context of credit reporting. Credit reports are subject to federal legislation which requires, among other things, that consumer reporting agencies (*e.g.,* credit bureaus) provide consumers with a copy of their credit report and follow reasonable procedures to assure maximum possible accuracy of information contained in the report.(236) The justification underlying this requirement is that information contained in the credit report may be used to make decisions that adversely affect consumers.(237) Thus, consumers have the right to see what information is in their credit file.

The individual reference services serve their customers -- entities who use information to take actions impacting data subjects -- and not the data subjects themselves. While there is an obvious incentive to give their customers accurate information, the individual reference services have less incentive to address concerns of data subjects.(238) The adverse effects on data subjects caused by inaccuracies in records maintained about them, including personal information gleaned from non-public sources or outdated, incomplete, or mismatched public records, can be much more severe than their impact on customers.(239) An information industry association argues that it is too burdensome to provide data subjects with access to their records.(240) However, the cost of providing consumers access could be passed on in the form of fees. Proponents of consumer access do not oppose the imposition of such fees, so long as they are reasonable.(241)

Providing consumers with access to records held about them is a first step toward ensuring that data is accurate. This access is meaningful only with a method in place that allows consumers to correct inaccuracies. To help ensure that records maintained about individuals are as accurate as possible, look-up services should also obtain information only from reputable sources and must implement a system that enables individuals to dispute and correct inaccuracies.(242) The industry maintains that look-up services are not able to change or delete information that is in a public record and therefore they cannot change or delete data they maintain that originated from public records.(243) This position assumes that public records information maintained by the look-up services mirrors the original public records, and overlooks the fact that public

records information may not be accurate once it is transferred from the custodian of public records and merged with other data. It may not be current. It may reflect transcription or transmission errors. Or, it may have been erroneously linked with the records of a different individual having the same or similar name.

D. Providing Consumers with the Ability to Opt Out or Opt In

Some privacy and consumer advocates assert that consumers should have the ability to make an informed choice as to whether to permit individual reference services to make their personal identifying information available.(244) This choice (or "consumer control") would necessarily take the form of either "opt in," requiring the look-up services to affirmatively obtain an individual's permission before making information about them available, or "opt out," permitting the look-up services to disseminate information about a particular consumer until the consumer instructs them otherwise. Only a select few individual reference services allow consumers to opt out of one or more of their databases.(245) Proponents of consumer control note that an opt out option is meaningless if consumers are unaware that a database exists.(246) Accordingly, some suggest that either an opt in option should be mandated,(247) or consumers should have the ability to opt out only once, through a universal system that affects all services.(248) Not all proponents of consumer control assert that the control should extend to public records; some support making public records information available regardless of consumer consent as long as the information is made available for free, and there is no legitimate economic incentive to exploit it.(249)

Although giving consumers control over the secondary use of their personal identifying information is an accepted fair information practice in several contexts,(250) here this approach is not without significant costs. In addition to individuals simply concerned about their privacy, those who would most likely choose to have their records excluded from the look-up services are those whom law enforcement agencies and other societally beneficial groups most want to find.(251) Users of the look-up services assert that the more complete the databases, the more useful they are in allowing such users to achieve their ends,(252) and that giving individuals complete control over information in this area likely would severely diminish the important societal benefits these services confer.(253)

One possible means of giving individuals control over their information without eliminating the industry's benefits would be to allow individuals to opt out of some, but not all, uses of their information.

E. Educating Consumers and Business

Many consumer and privacy advocates assert that consumers must be made aware of the existence of the individual reference services industry and of the available methods to control the use of their personal information (such as their ability to opt out of certain databases).(254) The concern that individuals should be informed about personal information record keeping systems has been repeatedly identified as an element necessary to protect consumer information privacy interests.(255) Several Workshop participants and commenters, including industry representatives, acknowledged that education about this industry is necessary.(256) One consumer advocate stressed that consumers need to learn about the risks of misuse of their personal information and not just the benefits of data collection and availability;(257) another noted that companies do not have an incentive to educate consumers about threats to their privacy.(258) Furthermore, privacy advocates argued that the industry should learn about the role that consumer privacy should play.(259)

VI. IRSG Proposal

In response to the Commission's announcement of this study, members of the individual reference services industry, including information suppliers and direct providers of commercial services (referring to themselves as the "Individual Reference Services Group" or "IRSG Group"), announced their intention to draft self-regulatory principles. Since the industry group's announcement, Commission staff has monitored and encouraged its progress.(260) Fourteen industry members have agreed to follow these self-regulatory principles (hereinafter the "IRSG Principles" or "Principles"). The signatories include companies that directly offer individual reference services, information vendors, and three national credit agencies.(261) The Principles set forth controls which address most concerns raised by the industry's dissemination of non-public information, defined as "information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.(262)

The Principles do not address the practices of online white-pages directory services, because the latter are not "commercial services" as contemplated by the Principles. However, this exclusion does not appear problematic. The majority of Internet white-pages services have already addressed consumer concerns by not displaying unlisted directory information, by permitting consumers to opt out, and by not allowing reverse address and telephone searches.(263) Furthermore, these services make available only directory information, not more sensitive identifying information such as Social Security number and date of birth.

A. The IRSG Principles

1. Restrictions on the Availability of Non-Public Information

The Principles impose restrictions on access to information obtained from non-public sources, or "non-public information" (*e.g.,* mother's maiden name and Social Security number obtained from "credit headers").(264) To the extent information obtained from a non-public source is publicly available, such as a home address that appears in a "credit header" but also is listed in the phone book, that information is *not* treated as "non-public." The Principles completely bar look-up services from making available certain non-public information, namely information gathered for marketing purposes.(265) Otherwise, the nature of information provided by an individual reference service and corresponding controls vary according to the category of customer. There are three categories of customers: "qualified subscribers," "professional and commercial users," and the general public. In general, customers that have less restricted access to non-public information ("qualified subscribers" and "professional and commercial users") are subject to greater controls. Conversely, the general public has more restricted access to non-public information and is subject to fewer controls. The particular categories of customers, the information available to them, and the corresponding controls are described below.

The Principles allow unrestricted distribution of certain non-public information only to "qualified subscribers." An entity can access services as a "qualified subscriber" only after: (1) the service conducts a reasonable review of the subscriber and its intended uses of the information; (2) the service determines that the intended uses are "appropriate;(266) (3) the entity agrees to limit its use and redissemination of such information to such "appropriate" uses; and (4) the entity agrees to terms and conditions consistent with the Principles.(267) Depending on the particular signatory, "qualified subscribers" might include law enforcement agencies and private investigators, and "appropriate" uses might include locating criminal suspects or the searching for missing children.(268)

The distribution of non-public information is more restricted for the category of "professional and commercial users." This category includes entities falling somewhere between qualified subscribers, who have a legitimate need for sensitive information, and the general public. "Professional and commercial users" can access certain non-public information if they use it in the normal course and scope of their business and profession, and if the use is appropriate for such activities. While they do not undergo the strict qualification process imposed on subscribers in the first category, they do not enjoy access to the same non-public information. They can access only truncated Social Security numbers (meaning a portion of the Social Security number has been replaced by "X"s), and month and year of birth (not full date of birth), and cannot access mother's maiden name or information that reflects credit history, financial history, or medical records. Furthermore, users in this category may access non-public information about children only for purposes of finding missing children.(269) At the same time, because members of this category are professional users whose professional use is linked to the need to access information, they can access more information than can the general public. Before granting access to non-public information to a "professional or commercial user," the services must: (1) establish that the user is a professional or commercial entity; (2) require the user to agree to terms and conditions consistent with the Principles; and (3) require the user to use the information to advance its business or professional purpose, and to limit any redissemination of such information to such uses, in accordance with the Principles.(270)

Depending on the company, examples of "professional and commercial users" might include lawyers seeking to locate potential witnesses, marketers assuring the accuracy of their potential customer lists, and banks seeking to detect fraud.

The third category, "general distribution," includes the general public. The Principles prohibit individual reference services from distributing to the general public certain non-public information such as Social Security number, mother's maiden name, birth date, credit history, financial history, medical records, or similar information, or any information about children. They also prohibit making available both unlisted telephone numbers obtained from sources other than public records and unlisted addresses obtained from the telephone company. However, services may make available unlisted addresses if they are obtained from sources other than the telephone company, such as the gas company. Furthermore, look-up services may not allow the general public to run searches using Social Security number as a search term.(271)

To protect the security of sensitive information, look-up services are required to maintain facilities and systems to protect information from unauthorized access. In addition to physical and electronic security, look-up services must require employees and contractors to sign confidentiality agreements and to be subject to supervision. The Principles require services to conduct system reviews at appropriate intervals to ensure that employees are complying with policies.(272)

2. Monitoring Use and Maintaining Audit Trails

The Principles require the look-up services to take reasonable steps to protect against the misuse of non-public information.(273) Each service must make available upon request an explanation of the uses of its non-public information it deems appropriate for "qualified subscribers," as well as an explanation of the types of "qualified subscribers" that can access such information.(274) The services must take reasonable steps to remedy abuses of the information by "qualified subscribers" and "professional and commercial users,(275) and must employ reasonable measures to ensure that the information is used appropriately.(276) Furthermore, individual reference services must maintain, for three years after termination of each subscriber's

relationship with the individual reference service, a record of the identity of each subscriber in these two categories, the types of uses employed by the subscriber, and the terms and conditions agreed to by the subscriber.(277) The look-up services are not required to maintain records of what information their users accessed.

3. Consumers' Access to Personal Information and Methods to Ensure Information Accuracy

Upon an individual's request, the Principles require a look-up service to provide copies of *non-public* information in its products and services that specifically identifies the individual.(278) The Principles do not compel the companies to provide individuals with copies of the *public* information that identifies them (*e.g.*, real estate records, court records, licenses, and other publicly available information). Rather, the Principles provide that each signatory shall inform individuals about the *nature* of public record and publicly available information that it makes available and the general sources of such information:(279) *i.e.,* not specific sources, but rather the entire universe of public records sources from which they create their databases.(280) As a result, under the Principles, individuals have no way of seeing files about them that reflect compiled public records information.

The Principles incorporate several measures to ensure that information products are accurate. First, identifying information may be acquired only from known, reputable sources whose data collection practices and policies are understood.(281) The services must take reasonable steps to help ensure the accuracy of the information.(282) Upon being informed of an inaccuracy by an individual, a service must either correct the inaccuracy or inform the individual of the source of the information. It must also tell the individual where a request for correction may be directed, if that information is reasonably available.(283) The Principles do not compel look-up services to correct inaccuracies reported by an individual about public record or publicly available information maintained by the services about that individual.

4. Ability to Opt Out

The Principles provide individuals with the ability to opt out of only "general distribution" of their non-public information.(284) Individuals may not opt out of distribution to "qualified subscribers" or to "professional and commercial users." Furthermore, signatories may not make available "unlisted" telephone numbers or addresses obtained from a telephone company.(285) If an individual has not opted out of a service's general distribution, however, the service is permitted to make available that individual's "unlisted" name and address if it obtains the information from sources other than the telephone company. Upon request, the signatories must also inform individuals of any other choices available to limit dissemination of their information.(286)

5. Consumer Education and Openness

The Principles require the individual reference services to educate users and the public about privacy issues associated with their services, about the types of services they offer, and about the Principles.(287) In addition, each service must make available a privacy policy statement that describes what information it has from what types of sources, how it is collected, the type of entities to whom it may be disclosed and the type of uses to which it is put.(288) The services must also notify consumers about their practices through Web sites, advertisements, or company- or industry-initiated educational efforts.(289)

6. Compliance Assurance

The enforcement program has two prongs. First, signatories' practices will be subject to a review by a "reasonably qualified independent professional service." That entity will determine whether a signatory is in compliance with the Principles, using criteria based upon the Principles.(290) The summary of the annual review will be made public. Second, the Principles provide that signatories who are information suppliers may not sell information to look-up services that do not comply with the Principles.

B. Analysis of IRSG Proposal

The record reflects opposing views as to the very notion of self-regulation. Supporters of self-regulation believe that industry should be given the opportunity to regulate its own practices, and that government action should be taken only if this approach proves ineffective.(291) Critics point to one central weakness with this approach: the lack of either incentive or mechanism for enforcement.(292) They also highlight several difficulties, such as influencing industry members who do not adhere to self-regulatory schemes,(293) sustaining a self-regulatory program once public attention wanes,(294) and addressing nuanced privacy-related issues.(295)

In determining whether the IRSG Principles offer a viable self-regulatory program, the Commission has assessed the extent to which the Principles can effectively implement controls similar to those set forth in Section IV above. These controls include: (1) limiting the availability of sensitive information; (2) monitoring use and maintaining audit trails; (3) allowing individuals to access records maintained about them and dispute inaccuracies; (4) giving individuals control over their information (provided this would not impede important public interests); and (5) educating consumers and business about information practices and privacy issues. Even if such controls are set forth in principle, the Commission believes that they are not meaningful without an effective mechanism to assure compliance and to influence the practices of the entire industry.

The Principles address the first control, limiting the availability of sensitive information, through the three-tiered customer category scheme. These access restrictions not only prohibit signatories from making available to the general public Social Security numbers, full dates of birth, and information about children (which are obtained from non-public sources and not otherwise publicly available), but also limit the extent to which established, professional entities can obtain this information. Furthermore, before signatories can provide unrestricted access to information, they must take measures to verify the identity of potential users and establish the legitimacy of their purposes.

The Principles address the second control, monitoring use and maintaining audit trails, in part by requiring that signatories take measures to protect against misuse of all non-public information. Signatories must ensure that the more potentially sensitive information, which is available only to "qualified subscribers" and "professional and commercial users," is used properly; if it is not being used properly, they must remedy misuses. Moreover, signatories have to keep track of the identities as well as the *types* of information (but not the actual information) accessed by these two categories of users.

With regard to the third control, individuals' access to their own information, signatories must allow individuals to access *non-public* records maintained about them and dispute inaccuracies. As to the fourth safeguard, consumer control, the Principles allow individuals to opt out of the general distribution of their *non-public* information, but not out of distribution to qualified,

professional, or commercial users. Finally, the Principles include the fifth control, education, by requiring signatories to notify consumers as to their information practices and to educate them about privacy issues related to their industry.

Most important, the IRSG Principles show promise for success in a critical area: the framework should assure compliance by both signatories and other members of the industry. The signatories characterize themselves as the "vast majority" of the industry that supplies information to commercial users.(296) Thus, the vast majority of the industry has agreed to annual compliance reviews -- an innovative step for a self-regulatory program, particularly as applied to information practices. Publicizing the results of compliance reviews performed on signatories (and their customers) by third parties, coupled with potential liability under the FTC Act and similar state statutes for non-compliance, should assure the signatories' compliance.(297) In instances where non-signatories' practices are inconsistent with the Principles, they will likely be unable to obtain non-public information easily to redisseminate through their services. Major suppliers of non-public information to this industry -- and the only primary suppliers of credit header information -- have agreed to sell only to companies whose practices are consistent with the Principles. Therefore, the Principles can be expected to have a beneficial impact on the practices of even those entities who are not signatories.(298)

The IRSG Principles fail, however, to incorporate all the suggested controls, and therefore do not address important concerns that have been raised about the industry. First, they provide essentially no limitations on the availability or uses of public records and publicly available information.(299) Accordingly, they do not limit the potential harm that could stem from access to and exploitation of sensitive information in public records and publicly available information. Second, the Principles fail to require individual reference services to maintain audit trails of the precise records accessed by each user, an important mechanism for identifying when an apparently legitimate entity obtains and uses information illegitimately and possibly the only mechanism that can link harm to the look-up services.(300) Third and most notably, the Principles fail to provide individuals with a means of accessing public records and other publicly available information maintained about them by individual reference services. The Commission is concerned that individuals have no way of discovering or correcting errors that may have occurred in the transcription, transmission, or compilation of this information.(301) Accordingly, the individuals cannot prevent, let alone identify, situations where that inaccurate information results in decisions which may adversely affect them. The Group is aware of this problem, and has stated that it will seriously consider conducting a study about the extent of relevant inaccuracies and related harm.(302)

Notwithstanding these shortcomings, the Principles have the potential to (1) curb misuse of non-public, personal identifying information; (2) address many of the relevant consumer information privacy concerns; and (3) significantly affect the practices of the entire individual reference service industry. The IRSG proposal is more comprehensive and far-reaching than any other voluntary, industry-wide program in the information sector. Members of the IRSG Group have made rapid and significant strides toward responding to consumers' concerns.

VII. Commission Recommendations

A. Recommendations Regarding the IRSG Principles

- **The Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles.**

The present challenge is to protect consumers from threats to their psychological, financial, and physical well-being while preserving the free flow of truthful information and other important benefits of individual reference services. The Commission commends the initiative and concern on the part of the industry members who drafted and agreed to the IRSG Principles, an innovative and far-reaching self-regulatory program. The Principles address most concerns associated with the increased availability of non-public information through individual reference services. With the promising compliance assurance program, the Principles should substantially lessen the risk that information made available through the services is misused, and should address consumers' concerns about the privacy of non-public information in the services' databases. Therefore, the Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles. *(For a detailed analysis of the IRSG Principles, see Section VI, supra.)*

- **The Commission looks to industry members to determine whether errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls.**

While the Commission believes the IRSG Principles address most areas of concern, certain issues remain unresolved.(303) Most notably, the Principles fail to provide individuals with a means to access the public records and other publicly available information that individual reference services maintain about them. Thus, individuals cannot determine whether their records reflect inaccuracies caused during the transmission, transcription, or compilation of such information. The Commission believes that this shortcoming may be significant, yet recognizes that the precise extent of these types of inaccuracies and associated harm has not been established. An objective analysis could help resolve this issue. The IRSG Group has acknowledged the Commission's position, and has demonstrated its awareness of this problem by (1) stating that it will seriously consider conducting a study of this issue and (2) agreeing to revisit the issue in eighteen months. The Commission looks to industry members to undertake the necessary measures to establish whether inaccuracies and associated harm resulting from errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls. *(For a detailed discussion of this issue, see Sections IV(B), V(C), supra.)*

B. Recommendations Regarding the Industry Generally

The Commission acknowledges that not every concern associated with the look-up services industry can be resolved by the individual reference services themselves. Rather, certain issues are within the control only of primary sources of information, other information providers, or of users of the information. Thus, understandably, the Principles cannot and do not address every concern associated with the industry. The Commission's recommendations with regard to concerns that cannot be addressed through the Principles are set forth below.

- **The Commission encourages 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.**

The Commission has found that the easy availability of sensitive, unique identifiers (*e.g.*, Social Security number, mother's maiden name, and date of birth) listed on public records increases the risk of serious harm. Given that information about such risks has surfaced only recently, public agencies may not have yet considered these risks in formulating their public records collection and dissemination practices. Thus, it is possible that certain government agencies may require and/or make available unique personal identifiers even though the collection and dissemination of that information is not essential to advance that agency's intended purpose. The Commission encourages 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. *(For a detailed discussion of this issue, see Sections II(2)(B)(1), IV(C), V(A)(2), supra.)*

- **The Commission urges online white-pages directory services that have not yet done so to implement important privacy safeguards, including not publishing unlisted directory information and allowing individuals to opt out of their databases.**

The Commission commends those online white-pages directory services that have voluntarily addressed consumer privacy concerns by allowing individuals to opt out of their database and by not publishing unlisted directory information. The Commission urges online white-pages directory services that have not yet done so to implement important privacy safeguards. *(For a detailed discussion of this issue, see Sections II(D), VI at 25, supra.)*

- **The Commission encourages users of individual reference services, where not otherwise required by law, to notify individuals voluntarily of adverse decisions based on information obtained through an individual reference service, and to disclose the source of such information, provided such disclosure would not hinder law enforcement or fraud prevention.**

The Commission has learned that users of look-up services may erroneously make adverse decisions affecting individuals because of inaccurate information obtained from individual reference services. Often, such individuals would have no way of knowing that information about them had been obtained, that it was inaccurate, or that it formed the basis for an adverse decision.(304) With adequate notification, such individuals could determine whether inaccurate information about them was disseminated, and, if appropriate, they could attempt to correct it. Accordingly, the Commission encourages users of individual reference services, where not otherwise required by law, to notify an individual voluntarily when they have made an adverse decision about that individual based on information obtained through an individual reference service. This voluntary adverse action notice should also disclose the source of the information on which the decision is based, provided such disclosure would not hinder law enforcement or fraud prevention. *(For a detailed discussion of this issue, see Section IV(B), supra.)*

- **The Commission recommends continued and enhanced consumer and business education.**

Finally, the Commission acknowledges the meaningful efforts undertaken by many privacy advocates, consumer groups, government agencies, and industry members to educate consumers and businesses about information privacy issues. The Commission looks forward to working with all of these groups to better inform consumers and businesses.

Endnotes

(1)In June of 1996, LEXIS-NEXIS released a locator product for its subscribers called P-Trak, and marketed the product's ability to find an individual's name, aliases, current and prior addresses, month and year of birth, and Social Security number. Roughly one week later, after a deluge of telephone calls from subscribers, the company provided individuals with the ability to have their information suppressed from the database ("opt out") and discontinued displaying Social Security numbers. Subscribers could still use a Social Security as a search term, to retrieve an individual's name and address. The following September, a message about P-Trak was posted to RISKS, an Internet discussion group that focuses on the risks of computer technology. Word of P-Trak then spread across the Internet and LEXIS-NEXIS was soon flooded with thousands of phone calls protesting, *inter alia,* the accessibility of Social Security numbers from the database. Stories about P-Trak and the public outcry appeared in both the *Washington Post* and the *Wall Street Journal*. *See* Mary J. Culnan, "Self-Regulation on the Electronic Frontier: Implications for Public Policy" in *Privacy and Self-Regulation in the Information Age*, US Dept. of Commerce, NTIA, June, 1997 at 50-51.

(2)The senators requested that the study encompass the collection, compilation, sale, and use of computerized databases that contain consumers' identifying information, without their knowledge. *See* Letter from Senators Larry Pressler, Richard H. Bryan, and Ernest F. Hollings to Commission (October 8, 1996). Separately, Congress requested the Board of Governors of the Federal Reserve System ("FRB") to conduct a study concerning the availability to the public of sensitive information about consumers, whether such information could be used to commit financial fraud, and if so whether its availability caused an undue potential risk of loss for depository institutions. 61 *Federal Register* 68,044 (December 26, 1996). The FRB released its report in March. Federal Reserve Board, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud, March 1997 [hereinafter "FRB Report"].

(3)The study was announced in the *Federal Register* last March. 62 *Federal Register* 10,271 (March 6, 1997). The Commission undertook this examination pursuant to Section 6 of the FTC Act, 15 U.S.C. § 46 (1997). In particular, Section 6(a) authorizes the Commission to "gather and compile information concerning . . . any person, partnership, or corporation engaged in or whose business affects commerce . . . ." *Id*. at § 46(a). Section 6(f) permits the Commission "to make annual and special reports to the Congress . . . ." *Id*. at § 46(f).

(4)See letter from Commission to Senator John McCain (February 28, 1997). In general, the FCRA (15 U.S.C. §§ 1681-1681u (1997)) governs the sale of consumer credit and other data compiled by agencies such as credit bureaus to parties evaluating individuals for credit, insurance, employment, or similar purposes. As set forth in detail below, many individual reference services offer a broad range of information, from purely identifying data, the primary focus of the study, to a vast array of other data gleaned from public records and other sources. Customers of the services use such information for locating individuals and verifying identities, as well as for many other purposes.

(5) Appendix A describes the Commission's information-gathering efforts in connection with the study.

(6)Other types of personal identifying information are described more fully in Section II.B. *infra*.

(7)See H. Jeff Smith, *Managing Privacy: Information Technology and Corporate America*. Univ. Press 1994, at 9, 178-79, 181-83. *See also,* United States Government, National Information Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure*, Draft for Public Comment (1997) at 1, 6; Carole Lane, *Naked in Cyberspace*, Pemberton Press 1997 at 44; Transcript of FTC Consumer Information Privacy Workshop, June 10, 1997 [hereinafter "Transcript"], Cerasale at 93-94; Varney at 95-96; Wenger at 102; Rotenberg at 104; Baity at 157-58. Unless otherwise indicated, footnote citations are either to the printed transcript of the June 10, 1997 Workshop or to public comments submitted pursuant to the March 6, 1997 *Federal Register* notice [hereinafter Comment, __ (Doc. No. __)]. The Workshop agenda can be found at Appendix B. A list of comments can be found at

Appendix C. All of these materials are on file at the Federal Trade Commission's Public Reference Room, File No. P974806, and are available online at *Federal Trade Commission, Consumer Information Privacy Workshop* (last updated December 5, 1997) 7 < ftc.gov/bcp/privacy2 >.

(8)Smith, *supra* n. 7, at 181-83; *see also* Transcript, Hendricks at 83-84.

(9)Smith, *supra* n. 7, at 7; Lane, *supra* n. 7, at 44.

(10)Smith, *supra* n. 7, at 7-9; Transcript, Dick at 78; Lane, *supra* n. 7, at 45.

(11)Smith, *supra* n. 7, at 178-79.

(12)Smith, *supra* n. 7, at 178-79.

(13)Id. at 8; Lane, *supra* n. 7, at 44. Today in the United States, 40 million computer information terminals sit on consumers' desks. Transcript, Dick at 126.

(14)Louis Harris & Associates and A. Westin, *Commerce, Communication, and Privacy Online, Report on National Survey of Computer Users*, 1997 [hereinafter "1997 Harris Survey"] at 1; Lane, *supra* n. 7, at 22.

(15)See Naom, *Privacy and Self-Regulation: Markets for Electronic Privacy* at n. 33 in *Privacy and Self-Regulation in the Information Age* (published by Dept. of Commerce, NTIA) 1997; *USA Today* Editorial "But this Nut's Tougher" 10/24/95. Eight companies report that together they employ over 5,000 employees to administer their individual reference services. Comments of Individual Reference Services ("IRSG") at 2 (Doc. No. 35). The whole information industry is growing rapidly. For example, in 1994, revenues from business information services exceeded $28 billion and, for the five years prior, the market for those services grew 6% annually. Comments of Information Industry Association ("IIA") at 6 (Doc. No. 32) (citing Veronis Suhler & Associates, *Communications Industry Forecasts*, 296, 305, 309 (9th ed. 1995)). The investigations industry, alone, has projected revenue to reach $4.6 billion by the year 2000 (four times the revenues in 1980). N. Bernstein, "Electronic Eyes: What the Computer Knows -- A Special Report; On Line, High-Tech Sleuths Find Private Facts," *New York Times*, September 15, 1997 at 1.

(16)See discussion of online reference services at Section 11.D. *infra*.

(17)In fact, apparently in response to this study, commercial entities that provide, directly or as suppliers to others, individual reference services, defined themselves as the individual reference service industry. *See* Comments of IRSG at 2 (Doc. No. 35); CDB Infotek at 5 (Doc. No. 20).

(18)In a promotional brochure sent out in July of 1997 to its government customers, Information America boasts that its People Finder database contains credit header information on "160 million individuals, 92 million households, 71 million telephone numbers, and 40 million deceased records." This promotional brochure is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

(19)When consumers offer this information, they generally may not realize that it may be made publicly available, transferred, or sold and then used in ways completely unconnected from the purpose for which they initially offer it.

(20)Comments of IRSG at 3 (Doc. No. 35).

(21)One noteworthy exception requires the Internal Revenue Service to disclose the contents of a tax return only in limited circumstances, such as in connection with conducting an income tax audit or locating the recipient of a tax refund. 26 U.S.C. § 6103 (1997). Another exception is a law prohibiting the

Census Bureau from publishing information that would identify a particular individual. 13 U.S.C. § 9 (1997).

(22)Lane, *supra* n. 7, at 251-79.

(23)See, e.g., Lane, *supra* n. 7, at 251-79.

(24)Id.

(25)About half the states restricted access to or use of voter registration records as of 1996. Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law*, Michie Law Publishers, Charlottesville, VA, 1996 at 54 (citing Robert Gellman, "Public Records: Access, Privacy and Public Policy" (1995) (unpublished)).

(26)Information America recently promoted its "FAA Airmen Directory" as containing, for all individuals registered to fly in the US, "information such as pilot's name, address, FAA region, certification class, medical certificate type and date of last medical exam." This promotional brochure is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

(27)Subject to its ability to withstand constitutional scrutiny, the federal Driver's Privacy Protection Act of 1994 ("DPPA"), effective as of September of 1997, may limit states' traditional practice of releasing motor vehicle records upon request. The DPPA requires that individuals be given some control over the release of their information, by limiting the circumstances under which the information can be disclosed unless "the motor vehicle department has provided in a clear and conspicuous manner on forms for issuance or renewal of operator's permits, titles, registrations, or identification cards, notice that personal information collected by the department may be disclosed to any business or person, and has provided in a clear and conspicuous manner on such forms an opportunity to prohibit such disclosures." 18 U.S.C. §§ 2721-2725 (1994). Two district courts have struck down the DPPA on Tenth Amendment grounds. *Condon v. Reno,* 972 F. Supp. 977 (D.S.C.1997), *appeal pending*; *Oklahoma v. United States*, 1997 U.S. Dist. LEXIS 14455 (W.D. Okla. 1997), *appeal pending*.

(28)Twenty-two states used the Social Security number as the driver identification number as of 1994. Testimony of Congressman James P. Moran, Before the House Subcommittee on Civil and Constitutional Rights on HR 3365, The Driver's Privacy Protection Act of 1993, 2/3/94, 1994 WL 14167988 (page unavailable online). Some states allow individuals the option of not using their Social Security number. *See, e.g.,* Va. Code Ann. § 46.2-342 (1997).

(29)FRB Report, *supra* n. 2, at 6.

(30) The sale of digitized records is providing governments with a new revenue stream. Illinois, for example, makes $10 million a year selling public records and Rhode Island makes $9.7 million selling Department of Motor Vehicle Records ("DMV") records alone. Bernstein*, supra* n. 15, at 1.

(31)Transcript, Wenger at 109.

(32)Id.

(33)Comments of IRSG at 5 (Doc. No. 35).

(34)Transcript, Hogan at 105-07; Comments of LEXIS-NEXIS at 2 (Doc. No. 18).

(35)Lane, *supra* n. 7, at 130-31; Comments of IRSG at 6 (Doc. No. 35); Transcript, Hanna at 129.

(36)See, *e.g.*, Comments of LEXIS-NEXIS at 2 (Doc. No. 18).

(37)See Lane, *supra* n. 6, at 57-59; Transcript, Lane at 48-50.

(38) Transcript, Lane at 51-52.

(39)For example, an information supplier could solicit information from individuals for the precise purpose of enabling them to be found through a look-up service. Some self-reported information, such as information voluntarily posted on one's own Web site, may be publicly available as well.

(40)See Transcript, Ford at 112.

(41)Equifax does not sell credit header information to private investigators and its locator products do not contain Social Security numbers. Transcript, Ford at 113-14.

(42)The FCRA allows credit reports to be distributed only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or similar purposes) under specified conditions (such as certification from the user), and provides for certain consumer rights in connection with the information maintained by credit reporting agencies (*see infra* n. 109). 15 U.S.C. §§ 1681-1681u (1997). A consumer reporting agency may not furnish medical information in connection with employment, credit, insurance, or direct marketing without the consent of the consumer. Section 604(g), FCRA, 15 U.S.C. §§ 1681b (1997).

(43)Comments of the DMA at 1(a) (Doc. No. 14). The DMA's Guidelines for Personal Information Protection indicate that personal information collected for marketing "should only be used" for marketing purposes and the DMA maintains that its Committee on Ethical Business Practice reviews complaints regarding the alleged use of marketing data for non-marketing purposes. Comment of the DMA at 1(b) (Doc. No. 14). Further, a Senior Vice President of the DMA has stated explicitly that magazine subscription lists and direct marketing lists may not be used by individual reference services. Transcript, Cerasale at 74. *See also* Transcript, Quarles at 238-39 (representing that Metromail's marketing information was not available to look-up services).

(44)See, e.g., Web sites of DigDirt, Inc., pimall.com/digdirt/index.html ; The Cat Midwest, http://spytaps.com/thecat/home1.html ; DocuSearch, http://www.docusearch.com . *See also* Transcript, Lane at 47, 50-51 (The reason unlisted phone numbers can be accessed through the Internet is that database operators purchase marketing lists, and these lists are increasingly being merged with other databases.)*See* Transcript, Reed at 71-73 (asserting that information products obtained from Metromail and sold by IRSC, an off-line reference service, originated from direct mail and magazine subscription lists); Reed at 245 (retracting his earlier statement and stating that he had been informed that Metromail has not sold information obtained from marketing transactions since 1994); Hanna at 76-77 (admitting that he did not know the current source of information products obtained from Metromail and First Data Corporation and sold by WDIA, an online reference service, but asserting that at least in the past they had originated from marketing information.) *See* Transcript, Reed at 71-73; Transcript, Hanna at 76-77. Transcript, Medine, Quarles, Reed at 244-245. cdb.com/public/services/locate.shtml on March 28, 1997 cdb.com/public/services/locate.shtml on March 28, 1997

(45)E.g., DigDirt, Inc. (visited November 26, 1997) < pimall.com/digdirt > (travel records and phone records); *The Cat* (visited November 26, 1997) < visi.com/thecat/missing1.html#sea1 > (utility records).

(46)For example, one individual reference service combines information from telephone directories and public records. Comments of LEXIS-NEXIS at 2 (Doc. No. 18).

(47)Comments of IIA (Doc. No. 32) at 18.

(48)Transcript, Reed at 74. To the extent an individual reference service provides customers with consumer reports (containing, *e.g.*, credit history, financial status, and employment background information), that entity may be acting as a "consumer reporting agency" subject to the obligations and restrictions set forth in the FCRA.

(49)E.g., Comments of Biggerstaff at 4 (Doc. No. 3); Comments of Privacy Rights Clearinghouse ("PRC") at 1 (Doc. No. 6). As these types of information become more widely available, they may become less useful as unique identifiers, and society may have to begin using other identifiers. Some under development include digital key signatures and biometrics such as retinal scans and digitized fingerprints. *See, e.g.*, Comments of Electronic Information Privacy Center ("EPIC") at 7 (Doc. No. 26).

(50)For example, at one time, one information provider, Metromail, provided access to the names, home addresses, and ages of children over a 900 number for three dollars a minute. This service has since been discontinued. Comments of EPIC at 6 (Doc. No. 26). In fact, Metromail along with certain other services, like LEXIS-NEXIS, have discontinued making available for wide commercial distribution non-public records about minors. Comments of IRSG at 12 (Doc. No. 35).

(51)DigDirt Inc. (visited on November 26, 1997) < pimall.com/digdirt/mo00016.htm >. Commission staff has not verified the accuracy of these representations.

(52)As discussed in more detail below, customers may have to pay subscription and monthly fees in addition to the costs of individual searches. *See* discussion at n. 59 *infra* and accompanying tex

(53)Typically, searches accessing higher numbers of databases that contain larger amounts of records cost more, as do searches for harder-to-obtain pieces of information.

(54)Although online commercial providers may not charge consumers directly for accessing information, they may otherwise profit from making the information available, such as through advertisements on their Web sites.

(55)For an in-depth discussion of which public records are available online, *see* Lane, *supra* n. 7, ch. 31.

(56)Comments of IRSG at 10 (Doc. No. 35) (discussing the practices of eight individual reference services).

(57)See, e.g., Comments of LEXIS-NEXIS at 3 (Doc. No. 18).

(58)Comments of CDB Infotek at 4 (Doc. No. 20); Comments of IRSG at 11 (Doc. No. 35) (discussing the practices of Database Technologies); Transcript, Hogan at 107-08.

(59)Comments of IIA, Appendix at 18 et. seq. (not paginated) (Doc. No. 32). One service, for example, charges an initiation fee of $130, a monthly fee of $30, and per-search charges ranging from $7 to $32. *Id.*

(60)Transcript, Hogan at 107-09; Abrams at 128.

(61)Notwithstanding the Commission's request for information, few companies volunteered specific information about their access limitations, contractual use limitations, or prices, presumably due to proprietary concerns.

(62)Comments of IIA at 22 (Doc. No. 32); Comments of IRSG at 11 (Doc. No. 35); Comments of NCISS at 3 (Doc. No. 11).

(63)Experian, for example, requires a nexus between the end user and the data subject when providing current and past addresses and Social Security numbers to organizations that use the information to locate or authenticate individuals. Transcript, Abrams at 114-15. For example, an insurance company would have a sufficient nexus to an uninsured individual who caused a car accident involving a motorist insured by the company. *Id.* at 116.

(64)Comments of IIA at 22 (Doc. No. 32); Comments of NCISS at 3 (Doc. No. 11); Transcript, Hogan at 107. For example, each of the four databases to which the National White Collar Crime Center subscribes examined the center's operation before granting it a subscription. However, the look-up services have not conducted any formal audits of the center's uses. Transcript, Belcher at 148-49.

(65)Comments of IIA at 22 (Doc. No. 32).

(66)Comments of IIA at 22-23 (Doc. No. 32).

(67)Comments of IRSG at 12 (Doc. No. 35). LEXIS-NEXIS' P-Trak database, for example, does not display Social Security numbers. Transcript, Welch at 21. Other services display Social Security number only on a truncated basis, *i.e.*, by replacing the last four digits with X's. Transcript, Hanna at 41. A customer, however, may use a Social Security number as a search term if she already knows that number. Transcript, Welch at 21; Hanna at 40- 41.

(68)Comments of IRSG at 12 (Doc. No. 35) (discussing the practice of LEXIS-NEXIS, Metromail, and other services, which avoid making available non-public information about minors, and the practice of Database Technologies and IRSC, which make such information available only for limited purposes, for example to search for missing children); Transcript, Welch at 22 (noting that LEXIS-NEXIS' P-Trak and P-Find databases do not contain information about individuals identified as being under the age of 18).

(69)Comments of IRSG at 12 (Doc. No. 35) (discussing, for example, LEXIS-NEXIS' practice of displaying an on- screen notice describing uses of the information that are covered by the FCRA)

(70)Transcript, Reed at 123; Abrams at 128.

(71)Comments of NCISS at 4 (Doc. No. 11); Comments of IRSG at 11 (Doc. No. 35) (discussing the practices of Database Technologies).

(72)Transcript, Dick at 59-60. A newspaper article reports that according to Jack Reed, president of an individual reference service and of NCISS, roughly 200 legitimate resellers of identifying information have sprung up on the Internet. Ed Mendel, "What Others Know Can Hurt You, *San Diego Union Tribune*, May 15, 1997 at A1. Privacy advocate Beth Givens, states that she finds a new online service everyday. Transcript, Givens at 189. Carole Lane, author of *Naked in Cyberspace*, estimates that the number of online individual reference services, if broadly defined, would be in the thousands. Transcript, Lane at 190.

(73)See, e.g.,Transcript, Hanna at 37 (discussing service available to general public over Internet through WDIA) and Lane at 44-47 (discussing services available to general public over Internet).

(74)DBT-Online reportedly offers this service to its 20,000 customers. Bernstein, *supra* n. 15, at 1.

(75)Comments of IRSG at 10 (Doc. No. 35) (discussing the practices of eight individual reference services).

(76)Transcript, Hanna at 38.

*(77)See, e.g.,*Transcript, Lane at 46 (discussing a service made available over the Internet only to subscribers of CDB Infotek).

(78)Transcript, Dick at 301.

(79)Id. at 60.

(80)E.g., Transcript, Panzera at 138; Belcher at 146; Baity at 158-59; Comments of the National Council of Investigation and Security Services ("NCISS") at 3 (Doc. No. 11); Comments of Archer at 2 (Doc. No. 22).

(81)See, e.g., Transcript, Belcher at 146; Comments of IRSG at 1 (Doc. No. 36). "Twenty percent of the population change address on an annual basis." Transcript, Abrams at 235

(82)Transcript, various participants at 136-60. For example, one service reports that the following entities subscribe to its services: FBI, IRS, Health Care Financing Administration, and the US Department of Justice. Comments of CDB Infotek at 1 (Doc. No. 20).

(83)E.g., Comments of USSS at 1 (Doc No. 28); Comments of National White Collar Crime Center ("White Collar Crime Center") at 1 (Doc. No. 33); Transcript, Panzera at 137-38; Belcher at 144-45; Baity at 158-59.

(84)Transcript, Baity at 158-59; Belcher at 154-55; Panzera at 137-38.

(85)Comments of White Collar Crime Center at 1 (Doc. No. 33).

(86)Transcript, Panzera at 137-38; Comments of USSS at 1 (Doc. No. 28).

(87)Comments of White Collar Crime Center at 1 (Doc. No. 33).

(88)See FinCEN (visited on December 5, 1997) <ustreas.gov/treasury/bureaus/fincen/faqs>; Transcript, Baity at 158.

(89) Transcript, Baity at 156-57. In addition to its financial database, FinCEN uses roughly fifteen commercial databases, and has access to almost all law enforcement databases. *Id.*

(90) In fact, FinCEN's analysts provide case support to more than 150 federal, state, and local agencies and issue approximately 8,000 intelligence reports each year. *FinCEN* (visited December 5, 1997) <ustreas.gov/treasury/bureaus/fincen/faqs>.

(91)Transcript, Baity at 157.

(92)Id.

(93)Comments of White Collar Crime Center at 1 (Doc. No. 33); Transcript, Belcher at 147.

(94)Contrary to the assertions of the individual reference services, some industry critics maintain that another private sector use -- marketing -- is what actually drives the industry. *E.g.*, Transcript, Sobel at 214. Again, databases used primarily for marketing fall outside the scope of this study.

(95)See Comments of IRSG at 13-15 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11); Transcript, J. Byrne at 207 (bank industry representative noting that the Secret Service is "great at investigating credit card fraud but that they can't do everything"); Transcript, Hulme at 228 (representative of NCISS

asserting that the private security sector is twice as large as the public security sector); Transcript, Jensen at 165-66 (representative of a non- governmental child support enforcement agency asserting that without the help of agencies like theirs, custodial parents in dire financial straits could have to wait a long time for services to be rendered by their government counterparts, and potentially jeopardize their children's health and safety); Comments filed by individual members of the private investigation and information industry (Doc. Nos. 39-243, 245-271) [hereinafter "Comments of Private Investigation Industry"] (stating that the free flow of information allows the public, who would otherwise not have the resources, to defend themselves without relying on government for help).

(96)See Comments of IRSG at 13-14 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (*e.g.,* Doc. Nos. 43, 47, 67, 78, 103, 141, 143, 149, 182, 197, 206); Transcript, J. Byrne at 207; Transcript, Jensen at 165-66 .

(97)Comments of CDB Infotek at 2 (Doc. No. 20); Comments of IRSG at 14 (Doc. No. 35).

(98)See Transcript, Reed at 121-22.

(99)Comments of National Retail Federation ("NRF") at 5 (not paginated) (Doc. No. 21); Transcript, Duncan at 205-07; Comments of GE Capital at 1 (not paginated) (Doc. No. 2); Comments of IRSG at 14 (Doc. No. 35).

(100)Comments of NRF at 5 (not paginated) (Doc. No. 21); Transcript, Duncan at 205-07; Comments of IRSG at 14 (Doc. No. 35).

(101)Comments of American Bankers Association ("ABA") at 2-3 (Doc. No. 1); Transcript, J. Byrne at 207-08.

(102)Comments of ABA at 3 (Doc. No. 1).

(103)Id.

(104)Id.

(105)Due diligence refers to a legal requirement compelling individuals to diligently verify certain information before taking various types of actions, *e.g.*, verifying the financial status of an entity before a merger or acquisition.

(106)Comments of IRSG at 9, 15 (Doc. No. 35).

(107)Transcript, Duncan at 206 (noting that credit grantors in retail industry use services in deciding whether to grant credit); Comments of ABA at 3 (Doc. No. 1) (noting that banks use services to ensure that potential bank employees have clean criminal records); Transcript, Reed at 195-96 (noting that the corporations use credit header information to detect misrepresentations on job applications); Transcript, Sobel at 214 (asserting that services are used to make employment, insurance, and credit decisions); Transcript, Givens at 182-84 (asserting that services are used to make employment decisions)

(108)Workshop participants and entities that submitted comments to the Commission were not clear as to whether credit and employment decisions are based on consumer reports (containing, *e.g.*, credit history, financial status, and employment background information). *See, e.g.*, Transcript, Duncan at 206 (retail industry representative referring to the information obtained from database services as a "credit report"); Comments of Independents Bankers Association of America ("IBAA") at 4-5 (not paginated) (Doc. No. 24) (bank association referring to individual reference services, including LEXIS-NEXIS, as "credit bureaus"); Transcript, Sobel at 214 (asserting that services are used to make employment, insurance, and credit decisions); Transcript, Givens at 182-84 (stating that services are used to perform

background checks on potential employees). This lack of clarity likely stems from the fact that certain individual reference services also act as credit bureaus. Transcript, Hanna at 39-41; Reed at 194. Such services, in addition to providing basic identifying information, also provide consumer reports pursuant to the requirements set forth in the FCRA. Transcript, Hanna at 39-41; Reed at 194.

(109)Under the FCRA, in such situations data subjects about whom adverse decisions are made are entitled, *inter alia*, to receive an adverse action notice stating the name, address, and phone number of the consumer reporting agency that provided the data leading to the action (Section 615, 15 U.S.C. § 1681m (1997)), to obtain all the information in the agency's file on them (Section 609, 15 U.S.C. § 1681g (1997)), and to dispute the accuracy or completeness of the information with the agency (Section 611, 15 U.S.C. § 1681i (1997)).

(110)E.g., Comments of IRSG at 9 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (Doc. No. 105); Comments of LEXIS-NEXIS at 6 (Doc. No. 18).

(111)Comments of LEXIS-NEXIS at 6 (Doc. No. 18).

(112)Comments of CDB Infotek at 2 (Doc. No. 20).

(113)E.g., Comments of IRSG at 9 (Doc. No. 35); Comments of CDB Infotek at 2 (Doc. No. 20); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (Doc. No. 105).

(114)E.g., Comments of IRSG at 9, 17-18 (Doc. No. 35); Comments of CDB Infotek at 2-3 (Doc. No. 20); Comments of LEXIS-NEXIS at 5 (Doc. No. 18); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (Doc. No. 105).

(115)E.g., Comments of NCISS at 2 (Doc. No. 11); Comments of IRSG at 13-19 (Doc. No. 35); Comments of Private Investigation Industry (Doc. No. 105).

(116)See Comments of NCISS at 2 (Doc. No. 11); Comments of IRSG at 15-19 (Doc. No. 35); Comments of Private Investigation Industry (Doc. No. 105).

(117)See Comments of IRSG at 15-19 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11).

(118)Comments of LEXIS-NEXIS at 6; Transcript, Edington at 221-22; Comments of IRSG at 19-20 (Doc. No. 35).

(119)Transcript, Hulme at 229; Allen at 317-18; Comments of Child Quest International at 1(Doc. No. 106).

(120)Comments of Childcare Checkpoint (Doc. No. 34).

(121)Comments of IRSG at 19 (Doc. No. 35).

(122)Transcript, Jensen at 161-64; Comments of Association for Children for Enforcement and Support ("ACES") (not paginated) (Doc. No. 4); Comments of IRSG at 15 (Doc. No. 35). One non-profit organization relies heavily on an offline service to enable mostly low-income, single mothers to track down current addresses for absent, non- paying parents. Comments of ACES at 1 (not paginated) (Doc. No. 4

(123)Id. at 2. This organization states that in the past ten years it has been able to assist over 25,000 families in finding non-paying parents using some type of computerized database, which translates into families collecting an average of $4,000 per year in child support. *Id.*

(124)Transcript, Jensen at 163-64.

(125)Transcript, Kirtley at 169; Comments of Reporters Committee for Freedom of the Press ("Reporters Committee") at 2 (Doc. No. 16).

(126)Transcript, Kirtley at 170-72; Comments of Reporters Committee at 3-4 (Doc. No. 16).

(127)Transcript, Kirtley at 180.

(128)Comments of IRSG at 18-19, 21 (Doc. No. 35); Comments of CDB Infotek at 3 (Doc. No. 20).

(129)Transcript, Reed at 121-22.

(130)Comments of IIA at 20 (Doc. No. 32).

(131)Comments of Junkbusters at 11 (Doc. No. 15).

(132)One potential means would be to sue a look-up service that provided inaccurate information on grounds of libel. However, such actions lie only if there is injury to a data subjects's reputation. Comments of Reporters Committee at 4 (Doc. No. 16). Furthermore, only in rare circumstances would the data subject learn of the inaccuracy and have the ability to trace it back to the look-up service.

(133)Survey results form 1978 to 1994 indicate that increasing numbers of consumers have expressed concern about threats to their personal privacy in America. Louis Harris and Associates, Inc., *Interactive Services, Consumers and Privacy* (conducted for *Privacy and American Business*) (1994) [hereinafter "1994 Harris Survey"] at 1; Louis Harris & Associates 1996 *Equifax-Harris Consumer Privacy Survey* (conducted for Equifax, Inc.) (1996) [hereinafter "1996 Harris Survey"]. In fact, in late 1996, this figure rose to 89%. *Hearing on "Electronic Payment Systems, Electronic Commerce, and Consumer Privacy Before the Subcomm. on Financial Institutions and Consumer Credit, House Comm. on Banking and Financial Services*, Sept. 18, 1997 (Statement of Dr. Alan F. Westin) [hereinafter "Westin Testimony"]. Yet another survey demonstrates that 80% of Americans feel that "[c]onsumers have lost control over how personal information about them is collected and used by companies." 1997 Harris Survey at xvii (reporting that 80% of computer users in 1997 and that 80% of all Americans in 1995 agreed with this statement). Survey research also indicates that people differ in their conception of privacy -- roughly 25% are "privacy fundamentalists" and do not want to disclose personal information in return for opportunities and benefits; about 20% have little or no concern and willingly disclose their information; and the majority evaluate their privacy concerns on a case-by-case basis. Westin Testimony; Federal Trade Commission's Bureau of Consumer Protection, *Staff Report*, "Public Workshop on Consumer Privacy on the Global Information Infrastructure," (December 1996) [hereinafter "FTC 1996 Privacy Report"] at n. 25 and accompanying text (citing Westin). The individuals who decide on a case-by-case basis consider the following types of factors: the nature of the benefit being offered in exchange for personal information; what potential misuses of this information can be made; and whether adequate safeguards are in place to protect their information. *Id.* For an in-depth discussion of laws recognizing information privacy interests, see generally Schwartz & Reidenberg, *supra* n. 25.

(134)A.R. Dowd, "Protect Your Privacy," *Money Magazine*, Aug. 1997 at 107.

(135)See, e.g., Transcript, Givens at 181-82; Grant at 197; Comments of Privacy Rights Clearinghouse ("PRC") at 1 (not paginated) (Doc. No. 6); Comments of EPIC at 11 (Doc. No. 26); Comments of CDT at 6 (Doc. No. 29

(136)See n. 1, *supra* and accompanying text; Comments of EPIC at 6 (Doc. No. 26); Comments of PRC at 1 (not paginated) (Doc. No. 6); Comments of CDT at 6 (Doc. No. 29).

(137)See Transcript, Hendricks at 321; L. Byrne at 211; Comments of EPIC at 8 (Doc. No. 26); Comments of PRC at 2 (not paginated) (Doc. No. 6); Lane, *supra* n. 7, at 45.

(138)Comments of EPIC at 8 (Doc. No. 26); *see also* Transcript, Berman at 91.

(139)Consumers whose information in the databases enables them to claim an inheritance or collect a judgment do directly benefit from the services, as may consumers whose database information allows them to be found by a long- lost relative or friend. Some consumers, however, may prefer not to be found at all.

(140)See Comments of PRC at 2 (not paginated) (Doc. No. 6); Comments of EPIC at 11 (Doc. No. 26); Comments of National Consumers League ("NCL") at 3 (Doc. No. 12). One notable exception is LEXIS-NEXIS, which allows consumers to opt out of its P-Trak database. Transcript, Glass at 67. Furthermore, LEXIS-NEXIS is now planning to allow consumers to access their identifying information maintained in its P-Trak and P-Find databases. Comments of LEXIS-NEXIS at 2 (Doc. No. 18A). These databases are two of the 7,000 databases that LEXIS- NEXIS maintains. Transcript, Welch at 19.

(141)E.g., Comments of Avrahami at 1 (Doc. No. 23); Comments of CDT at 3 (Doc. No. 29); Comments of EPIC at 7 (Doc. No. 26); Comments of Junkbusters at 7 (Doc. No. 15); Transcript, Wenger at 86; Grant at 198; Sarna at 309-10. *See also* 1996 FTC Privacy Report at n. 24 and accompanying text.

(142)Similarly, a significant number of Americans choose not to make their phone numbers publicly available. In 1996, 33% of Americans were reported to have unlisted phone numbers. Schwartz & Reidenberg *supra* n. 25 at 243.

(143)People tend to perceive comprehensive data profiles as more intrusive than disparate bits of information. Smith, *supra* n. 7, at 7-9.

(144)Comments of Biggerstaff at 6 (Doc. No. 3).

(145)E.g., Transcript, Sarna at 310; Comments of Junkbusters at 7 (Doc. No. 15).

(146)Comments of CDT at 3-4 (Doc. No. 29); Transcript, Dick. In fact in a recent survey, 28% of consumers said they refuse to disclose their income range for marketing purposes. B. Negus, "You're Not Welcome," *Direct Magazine*, June 15, 1996 at 61, 63-64. Again, services used primarily for marketing are beyond the scope of this study.

(147)"E.g., Comments of Biggerstaff at 7 (Doc. No. 3).

(148)Transcript, Rotenberg at 88. This shift in comfort level was demonstrated when the Social Security Administration, in response to a deluge of complaints, withdrew its service of providing consumers with their files over the Internet within three days of initiating the service. Transcript, Hendricks at 84, Rotenberg at 88. The Social Security Administration has since resumed this Internet service, providing less information than before, with more privacy and security protections in place. *Social Security Administration* (visited December 8, 1997) < http://www.ssa.gov >.

(149)E.g., Comments of CDT at 3-4 (Doc. No. 29).

(150) The public response to LEXIS-NEXIS making Social Security numbers available through P-TRAK is discussed at n. 1 *supra*. As mentioned above, a recent *Money Magazine* poll indicates that 88 % of respondents are concerned about the sale of their Social Security number and other sensitive identifiers. A.R. Dowd, *supra* n. 134, at 107. The 1994 Harris Survey found that over 60% of the population was concerned that their Social Security number would be misused in the future. Yet, another survey found that over 95% of the public object to the collection of their Social Security number for marketing

purposes. Negus, *supra* n. 146, at 61, 63-4. At the same time, however, consumers provide their Social Security numbers in many marketing transactions where this number is requested but likely not necessary, *e.g.,* in applying for membership at a video rental store.

One survey has found that consumers also object to marketers collecting the following types of information: age (44%); approximate annual income (81%); length of time spent living at current address (46%); names and ages of children in the household (77%); height and weight (62%); spending limit on credit cards (90%). Negus, *supra* n. 146, at 61, 63-

(151)See Comments of EPIC at 8 (Doc. No. 26); Comments of Biggerstaff at 6 (Doc. No. 3); Transcript, Sarna at 310; Sobel at 216-18; Comments of IBAA at 3 (not paginated) (Doc. No. 21). These risks are discussed further at Section IV.C. *infra*.

(152)Comments of Biggerstaff at 6 (Doc. No. 3).

(153)See, e.g., Transcript, Sarna at 310.

(154)Public Opinion Strategies, *A Telephone Survey of Adults in the Continental United States* (conducted for the National Association to Protect Individual Rights) (1993) at 4.

(155)1997 Harris Survey at xviii.

(156)1996 Harris Survey at 40.

(157)Id.

(158)Id.

(159)These examples are not as far-fetched as they may appear; the latter two are loosely based on complaints the Commission has received in the credit reporting area.

(160)See discussion at n. 107 and 109 *supra* and accompanying text.

(161)United States Government, National Information Infrastructure Task Force, Information Policy Committee*, Options for Promoting Privacy on the National Information Infrastructure*, Draft for Public Comment (1997) at 6.

(162)Transcript, Reed at 71; Lane*, supra* n. 7, at 53.

(163)Some LEXIS-NEXIS products, for example, display the following warning: "This data is compiled by a third party from multiple sources. INACCURACIES DO EXIST." (emphasis in original).

(164)Transcript, Hogan at 106.

(165)Comment of IIA at 21-22 (Doc. No. 32).

(166)E.g., Comment of IIA at 23 (Doc. No. 32); Transcript, Tobin at 274; Comments of Private Investigation Industry (*e.g.,* Doc. Nos. 42, 46-49, 51, 53, 55, 56, 58-64, 66-69).

(167) Lane, *supra* n. 7, at 53.

(168) *Id.* at. 25

(169)Id. at 53, 252. For example, a file may be out of place during the scanning process. *Id*. at 252.

(170)See Lane, *supra* n. 7, at 53. Harm from mismatched files can be devastating. For example, in a situation that involved a computerized database, although not necessarily a look-up service, a New York man was targeted for skipping child support payments to a son he did not have. Public Advocate for New York City, Annual Report (1997) at 5. After his wages and income tax refunds were withheld, a warrant was put out for arrest, and he was fired from his job, the man discovered that the child welfare authorities had confused his record with that of an individual with the same name who did owe child support. *Id*. The Computer Matching and Privacy Protection Act regulates the compilation of data from automated record systems (data matching) by the federal government. It addresses potential problems posed by the compilation of data. This act requires, *inter alia*, that federal agencies independently verify matched data before taking adverse action regarding data subjects and give data subjects the opportunity to challenge the data's accuracy, unless only certain limited information is relied on for certain purposes. 5 U.S.C. § 552a(p) (1997).

(171)E.g., Transcript, Reed at 123-24; Comments of Junkbusters at 20 (Doc. No. 15); Comments of EPIC at 11 (Doc. No. 26); Comments of Biggerstaff at 20 (Doc. No. 3); Comments of PRC at 2 (not paginated) (Doc. No. 6).

(172)Transcript, Glass at 68.

(173)Transcript, L. Byrne at 211.

(174) When an adverse action is based on information from a consumer report, the FCRA requires the *user* to pro vide the consumer with a notice that sets forth (1) the fact that adverse action has been taken in whole or part based on information contained in a consumer report; (2) the name, address, and phone number of the consumer reporting agency that provided the report; (3) a statement that the agency did not make the decision and can not provide the specific reasons for the adverse action; and (4) a notice of the rights provided consumers by the FCRA to (A) obtain a free copy of their credit file upon request within 60 days, and (B) dispute information in their file they believe is inaccurate or incomplete. FCRA, § 615, 15 U.S.C. § 1681m (1997). Furthermore, when credit is denied or the charge for credit increased based on information *bearing on a consumer's credit worthiness* from any source *other than a consumer reporting agency* (*e.g*., from a reference on a loan application or from information obtained through an individual reference service), section 615(b) requires that users, upon request, disclose to the consumer the nature of that information. FCRA, § 615(b), 15 U.S.C. § 1681m (1997). This is a more limited disclosure than the FCRA provides to a consumer who suffers adverse action based on a consumer report.

The Commission has brought actions against employers and creditors for failure to give consumers adverse action notices pursuant to Section 615 in the absence of consumer complaints, finding that wronged consumers have no way of knowing about such violations, and therefore would never know to complain. *See In re Aldi Inc.,* FTC Docket No. C- 3764 (1997); *In re Brunos, Inc.* FTC Docket No. C-3760 (1997); *FTC v. Bonlar Corp,* Inc., 97-C- 7274 (N.D. Ill. 1997); *In re Electronic Data Systems Corp*., FTC Docket No. C-3342 (1991); *In re Keystone Carbon Company*, FTC Docket No. C-3360 (1992); *In re The Kobacker Co*., FTC Docket No. C-3359 (1992); *In re Macy's Northeast, Inc.*, FTC Docket No. C-3362 (1992); *In re McDonnell Douglas Corporation*, FTC Docket No. C-3361 (1992).

(175)A computer hacker is an individual who wrongfully gains access to computerized data through technological means.

(176)In other cases, individuals who access the services for apparently legitimate reasons may use the information for what could be perceived as offensive, if not unlawful, purposes. Private investigators, for example, who access the services may engage in "pretexting," *i.e*., using information to pose as the data subject and thereby probe more deeply into that individual's affairs, *e.g*., to obtain an itemized telephone or credit card bill. Journalists may use the services to unearth and disseminate embarrassing facts about celebrities. An employer may use the databases to find answers he was not allowed to ask during a job

interview, including age and marital status. A lawyer may comb through a service's databases looking for potentially damaging information, unrelated to the case at hand, about opponents or their lawyers, in the hope of using the information to dissuade them from going forward with the case. (In fact, this very practice was alleged by individuals who had been harmed by an explosion at a Texaco oil refinery in a suit against Texaco and its agents. Bernstein, *supra* n. 15, at 1.) Finally, voyeuristic individuals may inquire into their neighbors' and coworkers' records for their own amusement.

(177)Comments of the Cuneo Law Group (Doc. No. 244). The prison had been subcontracted to do data entry in connection with a project for a prominent information vendor. *Id.*

(178)D. Szwak, "Theft of Identity: Data Rape," *Michigan Bar Journal*, March 1995; Comments of NCL at 2 (Doc. No. 12).

(179)J.K. Bloom, " Alleged Spree Highlights Danger of Identify Theft," *The American Banker*, June 3, 1997 at 1.

(180)Comments of NCL at 2 (Doc. No. 12); Comments of WorldPages at 6 (not paginated) (Doc. No. 271). A firewall is a combination of hardware and software that separates a local area network (LAN) into two or more parts, restricting outsiders to the area "outside" the firewall while protecting the information that is maintained "inside" the firewall.

(181)Comments of Junkbusters at 21 (Doc. No. 15); Transcript, Charney at 314.

(182)See, e.g., Transcript, Charney at 314. Even the Central Intelligence Agency's Web site proved to be vulnerable to a group of Swedish hackers. Transcript, Cattlet at 231.

(183)S. Singer, "Internet Opens Your Windows to Everyone; Invasion Sorely Tests Right to Be Let Alone," *Sun- Sentinel*, August 3, 1997 ("Local" Section) at 1A.

(184)B. Ward, "Online Identity Theft Crime's ?Growth Industry'," *The Ottawa Citizen*, September 15, 1997.

(185)Commission staff spoke to an agent at the FBI's C-Tech (computer technology) division who stated that the Computer Emergency Response Team, based out of Carnegie Mellon University, reported 406 incidents of wrongful access to information stored in computers in 1991; 773 in 1992; 1,334 in 1993; 2,342 in 1994; 2,412 in 1995; and 2,573 in 1996.

(186)Private communication from an agent at the FBI's C-Tech division.

(187)Transcript, Sobel at 214; Comments of PRC at 2-3 (not paginated) (Doc. No. 6); Comments of EPIC at 8 (Doc. No. 26); Comments of NYAG at 3-4 (Doc. No. 8); Comments of CDT at 5 (Doc. No. 29); *see* also Transcript of the FTC Meeting on Identity Theft held on Aug. 20, 1996 [hereinafter "FTC ID Theft Transcript"], on file at the FTC and available over the Internet at *Federal Trade Commission, Conferences* (last updated October 1, 1997) < ftc.gov/ftc/conferences.htm >. The FRB found that "fraud related to identity theft appears to be a growing risk for consumers and financial institutions, and the relatively easy access to personal information may expand the risk." FRB Report, *supra* n. 2, at 21. Identity theft is a crime in which an individual impersonates her victim, using the victim's identifying information, namely the victim's name, birth date, Social Security number, driver's license number, etc. Once the thief has the name and the Social Security number, she can easily obtain any other information she needs. *See, e.g.,* FTC ID Theft Transcript; Comments of PRC at 3 (not paginated) (Doc. No. 6). The imposter assumes the new identity and uses it to run up huge credit card bills, take out loans and mortgages, and kite checks between various fraudulent bank accounts, all backed by the victim's good name.

(188)Consumer liability associated with use of stolen credit cards is generally limited to $50. Truth in Lending Act, Section 133(b); 15 U.S.C. § 1643 (1997).

(189)Transcript, L. Byrne at 211.

(190)See Comments of MasterCard/Visa at 4 (Doc. No. 19); Comments of IRSG at 23 (Doc. No. 35); Comments of LEXIS-NEXIS at 7 (Doc. No. 18

(191)U.S. v. Roger Cullen and Cheryl Cullen, CR-97-56 (D. Del. 1997); Private communication from State of Delaware detective who investigated the case and arrested the defendants; Bloom, *supra* n. 179, at 1.

(192)Private communication from State of Delaware detective who investigated the case and arrested the defendants and from US Secret Service agent who prosecuted the criminals.

(193)Bloom, *supra* n. 179, at 1; Private communication from State of Delaware detective who investigated the case and arrested the defendants and from US Secret Service agent who prosecuted the criminals.

(194) Private communication from State of Delaware detective who investigated the case and arrested the defendants and from US Secret Service agent who prosecuted the criminals.

One attorney who specializes in identity theft cases informed Commission staff that many recent cases of identity theft have involved perpetrators and victims living in different parts of the country. He asserted that such evidence strongly suggests that identify thieves are beginning to exploit computerized data. Private communication from David Szwak, an identity theft attorney in Shreveport, LA.

(195)"Greidinger v. Davis, 988 F.2d 1345, 1354 (4th Cir. 1993) (cited in Schwartz and Reidenberg, *supra* n. 25 at 57 and in Comments of CDT at 5 (Doc. No. 29); *see also State ex Rel. Beacon Journal Pub. v. Akron*, 640 N.E. 2d 164, 169; 70 Ohio State 3d 605 (Ohio 1994) ("Thanks to the abundance of data bases in the private sector that include the SSNs of persons listed in their files, an intruder using an SSN can quietly discover the intimate details of a victim's personal life without the victim ever knowing of the intrusion.").

(196)See, e.g., Transcript, Hanna at 37; Welch at 27.

(197)It is not far-fetched to imagine a that a crook would be willing to invest a few hundred dollars in order gain access to a few hundred thousand (especially if the crook were charging the search to someone else's credit card in the first place).

(198)Transcript, Davies at 326-27, 335; Comments of IIA at 25 (Doc. No. 32); Comments of LEXIS-NEXIS at 7 (Doc. No. 18); Comments of IRSG at 21-24 (Doc. No. 35).

(199)"FRB Report, *supra* n. 2, at 21.

(200)See Comments of White Collar Crime Center at 2 (Doc. No. 33); Comments of IRSG at 21-24 (Doc. No. 35); Comments of LEXIS-NEXIS at 8 (Doc. No. 18). For an example of how this fraud detection takes place, see section III.B. *supra*.

(201)According to a *Money Magazine* poll, 21% of 35-44 year olds polled who had experienced an invasion in privacy later experienced stalking or other physical harassment. Dowd, *supra* n. 134, at 107; *see also* Comments of PRC at 3 (not paginated) (Doc. No. 6).

(202)Comments of PRC at 3 (not paginated) (Doc. No. 6).

(203)The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168055 (page unavailable online) (Statement of Donald L. Cahill, Legislative Chairman, Fraternal Order of Police). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

(204)The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168013 (page unavailable online) (Statement of David Beatty, Director of Public Affairs, National Victim Center). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806

(205)Certain companies have stopped making available information that identifies individuals as minors. Comments of IRSG at 12 (Doc. No. 35); *see supra* n. 50.

(206)The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168013 (page unavailable online) (Statement of David Beatty, Director of Public Affairs, National Victim Center). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

(207)Comments of PRC at 3 (not paginated) (Doc. No. 6).

(208)The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168055 (page unavailable online) (Statement of Donald L. Cahill, Legislative Chairman, Fraternal Order of Police). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

(209)See generally Comments of New York State Dept. of Law ("NYAG") (Doc. No. 8); Comments of CDT (Doc. No. 29); Comments of Biggerstaff (Doc. No. 3); Comments of EPIC (Doc. No. 26); Transcript, Sobel at 213-17; Givens at 181-87; Sarna at 309-13; Hendricks at 320-22.

(210)See US Dept. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (1973) [hereinafter "HEW Information Practices"], Safeguards, § I; 1996 FTC Privacy Report at 8-12; Secretary of Health and Human Services, Recommendations concerning the Confidentiality of Individually Identifiable Health Information (1997) [hereinafter "HHS Report"], § F; US Govt. Information Infrastructure Task Force, Information Policy Committee, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995) [hereinafter "IITF Principles"], § II.C.

(211)See Section IV.A., *supra*.

(212)E.g., Transcript, Sarna at 311.

(213)See Transcript, Biggerstaff at 331-32; Comments of Biggerstaff at 2,12 (Doc. No. 3).

(214)See supra n. 70 and accompanying text.

(215)Journalists take the position that journalists' rights to information should be coextensive with those of the general public. Transcript, Kirtley at 174.

(216)Transcript, Duncan at 205; J. Byrne at 207-08.

(217)See Transcript, Jensen at 166-67.

(218)Id.

(219)Comments of Biggerstaff at 2 (Doc. No. 3).

(220)Id.

(221)In fact, the Privacy Act compels federal agencies to store only personal information that is relevant and necessary. 5 U.S.C. § 552a(e)(1) (1997). Certain federal laws have implemented such limitations. For example, prior to 1995, the Postal Service provided individuals' change-of-address files to any person willing to pay the $3 fee. 59 *Federal Register* 67223 (1994). Now the Postal Service restricts the availability of this information to government agencies for official purposes, to persons legally empowered to serve process, and when necessary to comply with a court order. 39 CFR 265.6(d). In deciding to amend the regulation, the Postal Service expressed concern that "no postal interest is served by furnishing the information to persons who are seeking it for reasons unrelated to the use of the mails." 59 *Federal Register* 67223 (1994). Similarly, the DPPA, discussed *supra* n. 27, limits the information states can sell, by requiring states to check for a permissible business purpose before selling motor vehicle records, unless they have provided clear and conspicuous notice to consumers and an opportunity for them to opt out of having their information sold. 18 U.S.C. §§ 2721-2725 (1994

(222)See Comments of IRSG at 4 (Doc. No. 35).

(223)Id.

(224)Id.

(225)See, e.g., Comments of Biggerstaff; Transcript, Sarna at 310-11. The Office of the Information and Privacy Commissioner of British Columbia is currently examining this possibility. In particular, in its study of the impact of the accessibility of real estate assessment records online, that office is considering not displaying the name of the individuals who own the property because displaying the name does not advance the purpose of enabling the public to determine the value of real estate in a particular area. Yet, not displaying the name will enable property owners to keep their home address confidential if they so choose. Remarks of Commissioner David H. Flaherty, 1997 Privacy and American Business Conference, Washington, DC October 21, 1997.

(226)Transcript, Berman at 91.

(227)Comments of IIA at 20-21 (Doc. No. 32).

(228)See Comments of NCL at 2 (Doc. No. 12); Comments of CDT at 6 (Doc. No. 29); Comments of WorldPages at 6, 8 (not paginated) (Doc. No. 272).

(229)See, e.g., Comments of NCL at 2 (Doc. No. 12); Comments of WorldPages at 6 (not paginated) (Doc. No. 272); Comments of IBAA at 5 (not paginated) (Doc. No. 24).

(230)Comments of Biggerstaff at 12 (Doc. No. 3).

(231)Comments of GE Capital at 1 (not paginated) (Doc. No. 2); Comments of Biggerstaff at 12 (Doc. No. 3); *see also*, Transcript, Givens at 184; Comments of PRC at 5 (not paginated) (Doc. No. 6).

(232)See Transcript, Givens at 184; Comments of Biggerstaff at 12 (Doc. No. 3).

(233)One law enforcement representative noted that certain law enforcement functions could be undermined if audit trails were maintained and accessible. Transcript, Panzera at 143. One way to address this concern would be to keep confidential audit trails detailing uses by law enforcement.

(234)See Comments of Junkbusters at 20 (Doc. No. 15); Comments of NCL at 3 (Doc. No. 12); Comments of CDT at 2-3 (Doc. No. 29); Comments of *Privacy Times* at 1 (not paginated) (Doc. No. 9); Comments of PRC at 5 (not paginated) (Doc. No. 6); Comments of PRC at 2 (Doc. No. 16A); Transcript, Hendricks at 321-22; Rotenberg at 325-26 ("one of the most important privacy principles there is is the right to see information about yourself held by others.").

(235)See, e.g., HEW Report, Safeguards § III(2); 1996 FTC Privacy Report at 8-12; IITF Principles, § III.B; HHS Report, § I.G; Privacy Act, 5 U.S.C. § 552a(d) (1997); Cable Communications Policy Act, 47 U.S.C. § 551(a)(1) (1997

(236)The FCRA allows consumers to obtain a disclosure (in writing, unless other means are requested and available) of all the information in their credit file, if they request it and properly identify themselves. FCRA, Section 609, 15 U.S.C. §1681g (1997). Consumers are entitled to this disclosure at no cost if they ask for it within 60 days of any adverse action resulting from it, and at a current fee of no more than $8.00 in any case. FCRA, Section 612, 15 U.S.C. § 1681j (1997). The FCRA further requires consumer reporting agencies to follow reasonable procedures to assure maximum possible accuracy of the information concerning an individual about whom a consumer report relates. FCRA, Section 607(b), 15 U.S.C. § 1681e (1997).

(237) S. Rep. No. 517, 91st Cong., 1st Sess. 3 (1969) (legislative history to FCRA).

(238)See, e.g., Transcript, Grant at 201-03.

(239)This is especially true when an individual is denied an opportunity because her identifying information cannot be verified, or when an individual is deprived of an earned benefit because she cannot be found.

(240)Comments of IIA at 20-21 (Doc. No. 32).

(241)E.g., Transcript, Hendricks at 321; Comments of PRC at 3 (Doc. No. 16).

(242)See Comments of CDT at 3 (Doc. No. 29); Transcript, Hendricks at 321-22; Comments of PRC at 5 (not paginated) (Doc. No. 6); HEW Principles, Safeguards § III(6); HHS Report, § I.G.

(243)Comments of IIA at 21 (Doc. No. 32).

(244)E.g., Transcript, Dick at 126; Grant at 198-99; Avrahami at 306-07; Comments of CDT at 1-3 (Doc. No. 29); Comments of Junkbusters at 24 (Doc. No. 15); Comments of EPIC at 9 (Doc. No. 26); Comments of Avrahami at 2 (Doc No. 23). Some view this as the only option, because they believe that consumers are the owners of their personal identifying information. *E.g.*, Transcript, Grant at 198; Comments of Avrahami at 3 (Doc. No. 23).

(245)LEXIS-NEXIS allows its customers to opt out of its P-TRAK database but not its P-FIND database. Comments of LEXIS-NEXIS at 11 (Doc. No. 18). The majority of the online white-pages directory services allow individuals to opt out of their databases. Transcript, Dick at 304.

(246)Comments of EPIC at 11 (Doc. No. 26); Comments of NCL at 3 (Doc. No. 12).

(247)Comments of Avrahami at 2, 8 (Doc. No. 23); Comments of EPIC at 9 (Doc. No. 26).

(248)Comments of Avrahami at 8 (Doc. No. 23).

(249)E.g., Transcript, L. Byrne at 212-13; Avrahami at 307-08. Of course, identity theft and other types of fraud would remain as potential illegitimate economic incentives.

(250)See, e.g., HEW Report, Safeguards § II(3)*;* 1996 FTC Privacy Report at 8-12; IITF Principles, § II.D.

(251)See Transcript, Panzera at 140; Lane at 96-97; Allen at 318; Jensen at 203.

(252)See Transcript, Baity at 160.

(253)Comments of IIA at 20 (Doc. No. 32); Transcript, Panzera at 140; Lane at 96-97; Allen at 318; Jensen at 203; Comments of Private Investigation Industry (*e.g.,* Doc. Nos. 40-42, 44, 48, 50, 53-56, 58-64). Furthermore, in some cases, it makes more sense to allow consumers not to provide personal information in the first place, rather than opting out after the information has been transferred to the individual reference services, who are secondary providers

*(254)See e.g.,*Transcript, Hendricks at 321-22; Comments of PRC at 3 (Doc. No. 16A); Comments of IBAA at 2 (Doc. No. 24); Comments of CDT at 3 (Doc. No. 29).

(255)E.g., HEW Report, Safeguards § II*;* 1996 FTC Privacy Report at 8-12; IITF Principles, § II.B; HHS Report, § I.G.

*(256)E.g.,*Transcript, Abrams at 128, 25; Rotenberg at 132; Davies at 328; Comments of NCL at 4 (Doc. No. 12); Comments of Junkbusters at 31 (Doc. No. 15); Comments of PRC at 3 (Doc. No. 16A); Comments of IBAA at 2 (Doc. No. 24); Comments of CDT at 3 (Doc. No. 29). Interactive technology is one effective means of educating consumers, as well as a tool consumers can use to raise their voices in opposition to practices they find objectionable. *See* Transcript, Berman at 92.

(257)Comments of NCL at 4 (Doc. No. 12).

(258)Comments of Junkbusters at 31 (Doc. No. 15).

(259)See Transcript, Rotenberg at 132; Comments of EPIC at 15 (Doc. No. 26) (stating that the industry should be educated about legal duties, fair information practices, and new techniques to limit or eliminate the collection of personal data).

(260)A copy of the "Individual Reference Services Industry Principles" is attached as Appendix D. A copy of the official "Industry Principles -- Commentary" ("Commentary") is attached as Appendix E.

(261)The current signatories are: Acxiom Corporation; CDB Infotek, a ChoicePoint Company; DCS Information Systems; Database Technologies, Inc.; Equifax Credit Information Services, Inc.; Experian; First Data Solutions Inc.; Information America, Inc.; IRSC, Inc.; LEXIS-NEXIS; Metromail Corporation; National Fraud Center; Online Professional Electronic Network; and Trans Union Corp.

(262)"Principles at 1.

(263)Transcript, Dick at 300-04.

(264)Principle, § V. For a discussion of information obtained from non-public sources, see § II.B.3 *supra*.

(265)Principles, § II.B.

(266)""Appropriate," is defined as "reasonable under the circumstances reflecting a balance between the interests of individual privacy and legitimate business, governmental, and personal uses of information, including prevention of fraud." Principles at 1.

(267)Principles, § V.A.

(268)As discussed in note 42 *supra,* to the extent qualified subscribers have a "permissible purpose" under the FCRA, they may obtain information about an individuals' credit history, financial status, employment background, medical information, etc.

(269)Principles, § X.

(270)Principles, § V.

(271)Principles, § V.C.

(272)Principles, § VI.

(273)Principles, §§ V.A.2; V.B.3; V.C.2.

(274)Principles, § V.A.2.a.

(275)"Principles, §§ V.A.2.e; V.B.3.c.

(276)Principles, §§ V.A.2.d; V.B.3.b.

(277)Principles, §§ V.A.2.c.; V.B.3.d.

(278)Principles, § IX.A. Many look-up services had not followed this practice before the Principles. Transcript, Plesser at 260.

(279)Principles, § IX.B.

(280)The signatories explain their refusal to provide consumers with public records information about them by stating that it would be excessively burdensome to access the numerous public records databases for every inquiry (Commentary, App. E at 4) and that individuals can access public records that identify them at their source, the government custodian (Transcript, various participants at 265-68).

(281)Principles, § II.A.

(282)Principles, § III.

(283)Principles, § III.A.

(284)Principles, § VIII.

(285)Principles, § V.C.1.

(286)Principles, § VIII.

(287)Principles, § I.

(288)Principles, § VII.

(289)Principles, §VII.

(290)Principles, § XI; Commentary at 5.

(291)Transcript, L. Byrne at 315-16; Allen at 316; Comments of Etrust at 4-5 (now known as TrustE) (not paginated) (Doc. No. 10); Comments of Private Investigations Industry (Doc. Nos. 39-104, 106-243, 245-271); Comments of WorldPages at 8 (not paginated) (Doc. No. 272).

(292)Comments of *Privacy Times* at 1 (not paginated) (Doc. No. 9); Comments of PRC at 3 (Doc. No. 16A); Comments of NCL at 3 (Doc No. 12); Comments of EPIC at 13-14 (Doc. No. 26); Comments of Biggerstaff at 24 (Doc. No. 3); Comments of Avrahami at 8 (Doc. No. 23); Transcript, L. Byrne at 315-16; Biggerstaff at 287-89, Givens at 188; Rotenberg at 286, 324; Grant at 333; Culnan, *supra* n. 1, at 50-52. Marc Rotenberg recounted a situation in which a product, called Lotus Marketplace, containing marketing and credit information about consumers on a CD ROM was ready for release. The product, because it was a CD ROM, appeared to violate DMA self-regulatory guidelines requiring marketers to grant consumers the ability to opt out. Rotenberg claimed that the product was never released, not because DMA enforced the guidelines, but because 30,000 people complained through e-mail messages and the press. Transcript, Rotenberg at 283-86. Another example of self-regulatory guidelines not being enforced was cited by Jason Catlett, who noted a finding, reported in *DM News*, that thirty- eight percent of direct marketers were aware of fellow marketers renting house files without providing consumers notice or opt out options (a practice inconsistent with applicable self-regulatory guidelines). Transcript, Catlett at 293.

(293)Transcript, Hendricks at 322; Grant at 334; Culnan, *supra* n. 1, at 50-52. A related concern is that members of a given industry may not even know about that industry's self-regulatory guidelines. Transcript, Catlett at 293 (citing a finding, reported in *DM News*, that seventeen percent of direct marketers were not aware of the DMA's systems to allow consumers to opt out from receiving mail and telephone solicitations from its members).

(294)Transcript, Hendricks at 322.

(295)Transcript, Sarna at 311-12; Hendricks at 319; Rotenberg at 324.

(296)Transcript, Abrams at 241. Representatives of the Group have assured Commission staff that once the Principles have been finalized, the Group will find a mechanism to ensure that they are on-going, perhaps through involvement of a related trade association such as the IIA.

(297)Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (1997), prohibits unfair or deceptive acts or practices in or affecting commerce. By signing the Principles, a signatory represents that its information practices are consistent with the Principles. Subsequent action by the signatory that is not consistent with the Principles may thus be actionable under the FTC Act (or similar state statutes) as a deceptive act or practice. Of course, compliance with the Principles does not immunize the signers from scrutiny of their conduct under section 5.

(298)In implementing this aspect of the Principles, signatories should take care not to deny information to legitimate enterprises, particularly new entrants or others proposing to provide innovative, beneficial services. Accordingly, entities seeking access to information should be given a full and fair opportunity to demonstrate that their operations are consistent with the Principles or the underlying objectives of the Principles. By the same token, as the pace of technological change facilitates new approaches to the provision of individual reference services, the Commission urges that the IRSG ensure that the application of the Principles does not discourage innovative approaches that do not adversely affect consumers.

(299)Likewise, the provision that requires signatories to allow individuals to opt out of general distribution does not apply to information obtained from publicly available sources. As a result, if an individual opts out, that individual's address will be suppressed from databases created from non-public sources (*e.g.*, credit headers) but it may still be available through databases created from publicly available information (*e.g.,* DMV records).

(300)The Principles also fail to make signatories directly accountable to wronged individuals, a control important to several privacy advocates. Transcript, Avrahami at 305-06; Transcript, Rotenberg at 324; Comments of Avrahami at 8 (Doc. No. 23); Comments of Biggerstaff at 23-24 (Doc. No. 3).

(301)Commentary, App. E, at 4.

(302)Id.

(303)An audit trail requirement is also absent from the Principles. The Commission does not recommend that an audit trail be required at this time because the access restrictions appear to be sufficient to prevent misuse. If great harm does occur despite the Principles' limitations on the availability of sensitive identifying information, the Commission would urge the IRSG to revisit this issue.

(304) If an entity makes an adverse decision about a consumer based on information in a consumer report from a consumer reporting agency, the FCRA already requires, *inter alia*, that the entity provide the consumer with an adverse action notice. Furthermore, Section 615(b) requires a creditor that denies, or increases the charge for, credit based on information *bearing on a consumer's credit worthiness* from any source *other than a consumer reporting agency,* upon request, to disclose to the consumer the nature of that information. *See supra* n. 174.

Appendix A: Methodology

The Commission has gathered information about individual reference services in various ways. On March 6, 1997, the Commission issued a *Federal Register* Notice informing the public that the Commission would conduct this study. This notice announced that the Commission would hold a public workshop and requested public comment on certain specified issues and on any other issue of fact, law, or policy that could inform the Commission's study.(1) Additionally, FTC staff has met with dozens of individuals who requested to participate in the workshop. Staff has also spoken with entities whose views, experience, or information could better inform the Commission's analysis or help provide a balanced record. On June 10, 1997, the Commission held a one-day public workshop on individual reference services.(2) Panelists representing a broad range of view points and involved in varied aspects of the individual reference services industry responded to questions from the Commission about sources of and access to information contained in individual reference services' databases, the uses of that information and associated benefits and risks, and potential responses to address concerns.(3) In response to the *Federal Register* notice and the workshop, the Commission has received 272 formal written comments.(4)

---

(1) 62 *Federal Register* 10,271 (March 6, 1997). The *Federal Register* notice is included in Appendix A1.

(2)This workshop was part of a four-day public workshop held by the FTC to examine consumer information privacy in the emerging electronic marketplace. The workshop also examined current practices regarding the collection and use of personal information on-line, including information collected from and about children, self-regulatory efforts and technological developments since June 1996, and as unsolicited commercial e-mail.

(3)The Workshop agenda, including the names of all participants, is included in Appendix B. The transcript of the workshop is posted on the FTC's Web site at <ftc.gov/bcp/privacy2>.

(4)These comments are on file at the FTC and posted on the FTC's Web site at <ftc.gov/bcp/privacy2>.

Appendix C: List of Comments Submitted Pursuant to *Federal Register Notice*

Accipiter Doc. No. 007
Association for Children for Enforcement and Support (ACES)Doc. No. 005, Doc. No. 006
American Bankers Association (ABA) Doc. No. 004
American Marketing Association Doc. No. 001
James K. Archibald Doc. No. 022
Association of National Advertisers Doc. No. 030
Ram Avrahami Doc. No. 023
Robert Biggerstaff Doc. No. 003
CDB Infotek Doc. No. 020
Center for Democracy and Technology (CDT) Doc. No. 029
Childcare Checkpoint Doc. No. 034
Department of Treasury, United States Secret ServiceDoc. No. 028
Direct Marketing Association (DMA) Doc. No. 014
Dun & Bradstreet Doc. No. 036
Electronic Privacy Information Center (EPIC) Doc. No. 026
eTRUST Doc. No. 010
GE Capital/Montgomery Ward CRT Doc. No. 002
Independent Bankers Association of America (IBAA) Doc. No. 024
Individual Reference Services Group (IRSG) Doc. No. 035
Information Industry Association (IIA) Doc. No. 032
Junkbusters Corporation Doc. No. 015
LEXIS-NEXIS Doc. No. 018, Doc. No. 18A
National Consumers League (NCL) Doc. No. 012
National Council of Investigation & Security Services, Inc. (NCISS) Doc. No. 011
National Retail Federation (NRF) Doc. No. 021
National White Collar Crime Center Doc. No. 033
New York State Department of Law (NYAG) Doc. No. 008
Piper and Marbury Doc. No. 017
Privacy Rights Clearinghouse (PRC) Doc. No. 006, Doc. No. 016A
Privacy Times Doc. No. 009
Private Investigation Industry *see* pp. 2-5, Appendix CDoc. Nos. 037 - 271.
Reporters Committee for Freedom of the Press (Reporters Committee) Doc. No. 016
United States Department of Justice, Computer Crimes DivisionDoc. No. 031
United States Office of Consumer Affairs Doc. No. 025
VISA USA Doc. No. 019

Comments from the Private Investigation Industry

A.A. & Associates, Inc. Doc. No. 070
ABBA Investigations Doc. No. 256
Acta Investigations, Inc. Doc. No. 136
Adams' Investigations Doc. No. 049
Agency-One Investigations, Inc. Doc. No. 048
Alaska Investigators' Association Doc. No. 138
Alaska Shield Doc. No. 096
American Investigations & Security International Doc. No. 184
A.M. & Investigations, Inc. Doc. No. 125

Arbiter Investigations Doc. No. 153
Area Wide Investigations Doc. No. 180
Carlos S. Arias Doc. No. 060
Associated Global Insurance Services, Inc. Doc. No. 174
Attorneys' Investigative Consultants Doc. No. 113
Atwater Enterprises Doc. No. 185
Aurora Investigations, Inc. Doc. No. 142
Badger State Detective Agency Doc. No. 088
Badger State Investigative Service Doc. No. 079
Ball & Weed Doc. No. 143
Ball & Weed Doc. No. 182
Ball & Weed Doc. No. 261
Ball & Weed Doc. No. 271
Bates Investigations Doc. No. 152
Bayview Investigations Doc. No. 067
Benett Investigations Inc Doc. No. 078
Biscomb, P.I. Doc. No. 043
Black Knight Investigations Doc. No. 066
Bob Nesvick Investigative Services Doc. No. 087
Bombet, Cashio & Associates Doc. No. 069
Michael J. Brosnan P.D. Doc. No. 082
Cascade Pacific Detective Agency Doc. No. 047
Central Bail Bond Investigations Doc. No. 146
Cervantes & Associates, Inc. Doc. No. 109
Cervantes & Associates, Inc. Doc. No. 194
Citadel Protection & Investigations, Inc. Doc. No. 134
Corporate Investigative Services, Inc. Doc. No. 102
Countrywide Asset Investigators Doc. No. 123
C.R. Cochran & Associates Doc. No. 084
Cynthia Erdelyi Investigations, CPI, CIP Doc. No. 141
Data Research, Inc. Doc. No. 259
Dameron Investigative Services Doc. No. 193
Daniel & Nicolai Doc. No. 265
David C. Anmahian & Associates Doc. No. 051
DCR Enterprises Doc. No. 177
Delta Investigations Doc. No. 081
Steven E. Detata Doc. No. 155
Dial Services, Inc. Doc. No. 089
DLS Investigations Doc. No. 139
Don Malone & Associates, Inc. Doc. No. 149
Darryl Drew Doc. No. 156
Eagle Information Service Doc. No. 057
Eagle Investigations Doc. No. 072
Edie Lee & Associates Doc. No. 192
Edward R. Kirby & Associates, Inc. Doc. No. 071
Ellis Investigations Doc. No. 115
EX-CEL Investigations Doc. No. 120
EX Fed Investigative Services, Inc. Doc. No. 173
Factfinders Doc. No. 094
Factfinders Doc. No. 122
William E. Fason, P.I. Doc. No. 075
Five Rivers Investigations Doc. No. 074
Flynn & Associates Doc. No. 179
Flynn & Associates Doc. No. 187
Forensic Analysts Investigations Doc. No. 129
Arthur J. Forster Doc. No. 099
Gerald Adams & Associates, Inc. Doc. No. 145

Global Intelligence Network, Inc. Doc. No. 045
Global Intelligence Network, Inc. Doc. No. 269
Gradoni & Associates Doc. No. 255
Gray Security, Inc. Doc. No. 140
Joseph T. Grills Doc. No. 103
Alan Grover Doc. No. 257
G.W. Mack Investigations Doc. No. 158
Haberkern & Company Doc. No. 106
Hans de Haas & Associates, Inc. Doc. No. 083
Henderson & Associates Doc. No. 264
M. Randall Hicks Doc. No. 098
HUB Enterprises, Inc. Doc. No. 110
IAI Investigative Associates, Inc. Doc. No. 151
Information Please Doc. No. 189
Information Services Doc. No. 266
Information Services Investigations, Inc. Doc. No. 175
International Management Assistance Corporation Doc. No. 095
International Research Services, Inc. Doc. No. 112
Investigative Dynamics, Inc. Doc. No. 117
Invex Doc. No. 114
ION Incorporated Doc. No. 076
J.L. Fry Research & Investigations Doc. No. 073
JMK Investigations Doc. No. 254
John W. Palich Investigations Doc. No. 131
JR Investigations Doc. No. 077
JR Investigations Doc. No. 178
J.W. Strelec Investigations Doc. No. 144
James L. Kellner Doc. No. 085
Kellogg Investigation Services Doc. No. 157
Klopper Investigations Doc. No. 119
Krisztina Reports, Inc. Doc. No. 061
Krotzer Legal Investigations Doc. No. 065
Langhammer & Associates, Inc. Doc. No. 080
Lassen Investigative Services Doc. No. 093
Legal Research Services Investigations, Inc. Doc. No. 053
Litigation Assistance Work Doc. No. 172
L. Michael Connelley & Associates Doc. No. 176
Management Protection Services Doc. No. 253
MarKahn Co. Doc. No. 137
John F. Matula Doc. No. 126
MG Investigations Doc. No. 263
Al Morris Doc. No. 171
NASA One Services Doc. No. 181
NationsBank Doc. No. 160
Ed Nickel Doc. No. 038
Noragon & Associates Doc. No. 042
N. R. Cochran & Associates Doc. No. 166
Pacific Investigations Doc. No. 165
Paladin Investigations Doc. No. 054
Perrin Investigative Service Doc. No. 068
PFC Information Services, Inc. Doc. No. 190
Steven H. Phelps Doc. No. 147
Charles Pollard Doc. No. 154
P&R Executive Services Agency Doc. No. 133
P&R Executive Services Agency Doc. No. 163
Professional Inquiry, Inc. Doc. No. 092
Professional Investigative Consultants Doc. No. 183

Professional Investigators & Security Association Doc. No. 162
Protec Doc. No. 127
R. A. Heales & Associates, LTD Doc. No. 059
Carl S. Raphael, P.I. Doc. No. 052
Ray, McChristian & Jeans Doc. No. 191
RJC & Associates Investigations Doc. No. 086
R.J.N. Investigations, Inc. Doc. No. 124
R.J. Slepski Investigations, Inc. Doc. No. 118
Scott I. Ross Doc. No. 111
Ruffin & Associates Doc. No. 178-2
Saraceno Investigations Doc. No. 044
Security Solutions, Inc. Doc. No. 148
Scope Investigative Network Doc. No. 260
Shimrak Investigations Doc. No. 104
Skyhawk Investigations Doc. No. 116
Sleuth, Inc. Doc. No. 100
Sleuth Fox Investigations Doc. No. 064
Special Inquiry Company Doc. No. 268
Specialized Investigations Doc. No. 055
Specialized Investigations, Inc. Doc. No. 132
Steele Investigation Agency Doc. No. 168
Strasburger & Price, L.L.P. Doc. No. 186
Superior Service Bureau Doc. No. 063
Tactical Investigative Services Doc. No. 039
Tamara Thompson Investigation Doc. No. 050
Target Investigation Service Doc. No. 267
Technical Surveys Consulting Doc. No. 258
Texas Investigative Network, Inc. Doc. No. 150
Texas Judgment Recovery Co., Inc. Doc. No. 161
The Knorok Detective Agency Doc. No. 164
Thistle Investigation Services Doc. No. 270
Topp Notch Investigations Doc. No. 046
Trace Investigations Doc. No. 121
Trace Investigations Doc. No. 135
Universal Investigations, Inc. Doc. No. 159
Universal Protective & Investigations, Inc. Doc. No. 090
Video Trackers, Inc. Doc. No. 058
Vinson Detective Agency Doc. No. 050-2
Vinson Detective Agency Doc. No. 056
Vinson Detective Agency Doc. No. 108
W. A. Haag & Associates Inc. Doc. No. 091
Wallace Investigations Doc. No. 040
Walter Markely Investigations, L.C. Doc. No. 167
We Investigate, Inc. Doc. No. 170
Cal West Doc. No. 107
West Shield Investigations Doc. No. 188
Whitley Security and Investigations Doc. No. 252
Wilcox & Associates Doc. No. 128
William Sykes & Associates Doc. No. 097
Wind River Public Safety Services Doc. No. 062
Wood & Tait Doc. No. 041
World Investigations Doc. No. 101
Zrod Investigations Doc. No. 130

262 Jointly Filed Comments from Individual Members
of Private Investigation Industry Doc. No. 105

For more information about this report, please contact its principal author:
Lisa Rosenthal
Federal Trade Commission
Division of Credit Practices
6th & Pennsylvania, NW
Room S-4429
Washington, DC 20580

by phone: (202) 326-2249 or by electronic mail: lrosenthal@ftc.gov

Documents

File

Appendix D: IRSG Principles (49.93 KB)

File

Appendix E: Industry Principles -- Commentary (45.6 KB)

FINAL — DECEMBER 15, 1997

INDIVIDUAL REFERENCE SERVICES INDUSTRY PRINCIPLES

PREAMBLE:

The following principles were developed by members of the individual reference services industry to respond, as an industry, to heightened interest in the industry's practices. The principles represent good practices that the undersigned companies agree to support as part of their operating practices. While it may take up to a year for some principles to be implemented filly, other principles are already part of the operating practices of the undersigned companies.

SCOPE:

These principles apply to individual reference services, which are commercial services that directly or as suppliers to others provide information that assists users in identifying individuals, verifying identities and locating individuals for various purposes.

DEFINITIONS:

- *Public Record Information:* Information about or related to an individual which has been obtained originally from the records of a federal, state, or local governmental entity that are open for public inspection.

- *Publicly Available Information:* Information about an individual that is available to the general public from non-governmental sources such as telephone directories, classified ads, newspaper reports, publications, or other forms of information.

- *Non-Public Information:* Information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.

- *Appropriate or Appropriately:* Describes actions or uses that are reasonable under the circumstances reflecting a balance between the interests of individual privacy and legitimate business, governmental, and personal uses of information, including prevention and detection of fraud.

PRINCIPLES:

I. *Education:* Individual reference services shall individually and through their industry groups make reasonable efforts to educate users and the public about privacy issues associated with their services, the types of services they offer, these principles, and the benefits of the responsible flow of information.

II. *Reputable Sources:* Individually identifiable information shall be acquired from only sources known as reputable in the government and private sectors.

A. Reasonable measures shall be employed to understand an information source's data collection practices and policies before accepting information from that source.

B. Individually identifiable information that is collected for marketing purposes shall not knowingly be purchased, sold or retained for creating or inclusion in individual reference services, unless it is PUBLIC RECORD INFORMATION or PUBLICLY AVAILABLE INFORMATION; its use is specifically permitted by law; or it is collected with notice to the individual that such information will be used for inclusion in individual reference service products.

III. *Accuracy:* Reasonable steps shall be taken to help assure the accuracy of the information in individual reference services. The goal of individual reference service products is to furnish customers with accurate reproductions of information.

A. When contacted by an individual concerning an alleged inaccuracy about that individual, the individual reference service, as APPROPRIATE, shall either correct any inaccuracy or inform the individual of the source of the information and, if reasonably available, where a request for correction may be directed.

B. The individual reference service's commitment to furnish users with reasonably accurate reproduction of information in PUBLIC RECORD INFORMATION systems does not permit alteration of the substantive content of PUBLIC RECORD INFORMATION products or services.

IV. *Public Record and Publicly Available Information:* PUBLIC RECORD INFORMATION and PUBLICLY AVAILABLE INFORMATION shall be usable without restriction unless legally prohibited.

V. *Distribution of Non-Public Information:* Except as provided in section IX, NON-PUBLIC INFORMATION will be distributed only according to the criteria set forth below. The nature of NON-PUBLIC INFORMATION being requested and the intended uses of such information shall determine the level of review of the subscriber. Companies who supply information covered by this section to individual reference services shall provide such information only to individual reference services that adopt or comply with these principles.

A. *Selective and Limited Distribution of Non-Public Information:* Individual reference services may distribute NON-PUBLIC INFORMATION without restriction of its contents only to qualified subscribers.

1. Qualified subscribers for the selective and limited distribution of NON-PUBLIC INFORMATION must satisfy the following conditions:

   a. The subscribers must state their APPROPRIATE uses for such information.

   b. The subscribers must agree to limit their use and redissemination of such information to such APPROPRIATE uses.

   c. The subscribers shall be reasonably identified and meet qualification requirements that establish them as APPROPRIATE users of the information and agree to terms and conditions consistent with these principles prior to accessing the information.

2. Each individual reference service shall take reasonable steps to protect against misuse of NON-PUBLIC INFORMATION distributed pursuant to this subsection which will include:

   a. Each individual reference service shall make available upon request an explanation of what uses of its information are APPROPRIATE and to which types of qualified subscribers such information is available.

   b. Individual reference services shall conduct a reasonable review of the subscriber and its intended uses of the information prior to making NON-PUBLIC INFORMATION available to the subscriber.

   c. Individual reference services shall maintain a record of the identity of subscribers, the types of uses, and the terms and conditions agreed to by the subscriber for three years after termination of each subscriber's relationship with the individual reference service.

   d. Reasonable measures shall be employed to help assure that qualified subscribers use NON-PUBLIC INFORMATION APPROPRIATELY.

   e. Individual reference services shall implement reasonable mechanisms to remedy subscriber abuses of the information.

B. *Commercial and Professional Distribution of Non-Public Information:* Individual reference services, when they limit the NON-PUBLIC INFORMATION content of their

products or services as set forth below, may distribute such products or services only to established professional and commercial users who use the information in the normal course and scope of their business or profession and the use is APPROPRIATE for such activities.

1. NON-PUBLIC INFORMATION products or services distributed pursuant to this subsection shall not include:

a. Information that reflects credit history, financial history, medical records, mother's maiden name identified as such, or similar information;

b. Certain information like social security number and birth information unless truncated in an APPROPRIATE and industry consistent manner.

2. Users shall agree to terms and conditions consistent with these principles prior to accessing the NON-PUBLIC INFORMATION, shall agree to use such information solely in the normal course and scope of their business or profession and that the use is APPROPRIATE for such activities and that they shall limit their use and redissemination of such information to such uses and in accordance with these principles.

3. Individual reference services shall take reasonable steps to protect against misuse of the NON-PUBLIC INFORMATION distributed pursuant to this subsection which will include:

a. If not previously established, the individual reference service shall take reasonable steps to identify the user and to establish the user as an established professional or commercial entity.

b. Reasonable measures shall be employed to help assure that commercial and professional customers use NON-PUBLIC INFORMATION APPROPRIATELY.

c. Individual reference services shall implement reasonable mechanisms to remedy subscriber abuses of the information.

d. Individual reference services shall maintain a record of the identity of subscribers and the terms and conditions agreed to by the subscriber for three years after termination of each subscriber's relationship with the individual reference service.

C. General Distribution of Non-Public Information: Individual reference services, when they limit the NON-PUBLIC INFORMATION content of their products or services as set forth in this subparagraph, may distribute such products or services to any person.

1. NON-PUBLIC INFORMATION distributed pursuant to this subparagraph shall not - knowingly include information that reflects social security number, mother's maiden name identified as such, non-published telephone number, or non-published address information obtained from telephone companies, birth information, credit history, financial history, medical records, or similar information, nor will the service be retrievable by a social security number.

2. The individual reference service shall take reasonable steps to protect against the misuse of NON-PUBLIC INFORMATION.

VI. *Security*: Individual reference services shall maintain facilities and systems to protect information from unauthorized access and persons who may exceed their authorization. In addition to physical and electronic security, individual reference services shall reasonably implement:

A. Employee and contractor supervision-Employees and contractors shall be required to sign confidentiality agreements and be subject to supervision.

B. Reviews—System reviews shall be made at APPROPRIATE intervals to assure that employees are complying with policies.

VII. *Openness:* Each individual reference service shall have an information practices policy statement that describes what types of information it has, from what types of sources, how it is collected, the type of entities to whom it may be disclosed and the type of uses to which it is put, and shall make its policy statement available upon request. Consumers shall be notified about these practices in various ways such as:

1. Web sites;

2. Advertisements; or

3. Company or industry-initiated educational efforts.

VIII. *Choice:* Each individual reference service shall upon request inform individuals of the choices, if any, available to limit access or use of information about them in its data base, provided, however, that in the case of NON-PUBLIC iNFORMATION distributed to the general public (section V.C of these principles), an individual reference service shall provide an opportunity for an individual to limit the general public's access or use of such NON-PUBLIC INFORMATION.

IX. Access: Upon request and reasonable terns, an individual reference service shall:

A. Inform an individual about the nature of PUBLIC RECORD and PUBLICLY AVAILABLE INFORMATION that it makes available in its products and services and the sources of such information;

B. Provide individuals with NON-PUBLIC INFORMATION contained in products and services that specifically identifies them and that are distributed as part of an individual reference service to users under section V. of these Principles unless the information was obtained on a limited use basis from a governmental agency or if its disclosure is limited by law or legally recognized privilege; and

c. Direct individuals to a consumer reporting agency regulated by the Fair Credit Reporting Act where such agency is the source of the information about the individual.

X. *Children:* Where an individual is identified in the product or service as being under the age of 18, no NON-PUBLIC INFORMATION about that individual shall be provided for other than selective and limited distribution purposes or for the purposes of locating missing children.

XI. *Assurance of Compliance:* The signers of these principles shall have completed within 15 months of the effective date of these principles. and on a periodic basis thereafter, at least once every year, an assurance review done by a reasonably qualified independent professional service. The independent professional service shall apply assurance criteria consistent with these principles and approved by the signers as a group. Individual referenceservices shall have a reasonable opportunity to respond to any concerns expressed in such assurance review. A summary reflecting both the [original] report and any subsequent actions taken or response made by the company shall be publicly available.

PLEDGE:

The undersigned companies pledge to introduce and follow the above industry principles at the earliest practicable opportunity or by December 31, 1998, whichever is sooner.

Acxiom Corporation
CDB Infotek, a ChoicePoint Company
DCS Information Systems
Database Technologies, Inc.
Equifax Credit Information Services, Inc.
Experian
First Data Solutions Inc.
Information America, Inc.
IRSC, Inc.
LEXIS-NEXIS
Metromail Corporation
National Fraud Center
Online Professional Electronic Network
Trans Union Corporation

Individual Reference Services Group

FINAL — DECEMBER 15, 1997

INDUSTRY PRINCIPLES — COMMENTARY

BACKGROUND:

The Individual Reference Services Group (IRSG) is composed of leading companies of the individual reference services industry. In recognition of the heightened interest in issues related to their services, the IRSG has developed self-regulatory principles. The focus of these principles is non-public information; that is, information about an individual that is of a private nature and not generally available to the public nor obtained from a public record. Signatories to these principles include individual reference services, as well as those companies that supply information to such services.

Individual reference services provide information that identifies or locates individuals, These services provide important societal benefits, For example, information obtained from these services helps locate witnesses to crimes and parents who are delinquent in their child support payments, and assists in important governmental and business functions such as fraud prevention and detection. The principles do not apply to functions other than identifying or locating individuals or verifying individual identities, For instance, database services of newspaper archives, or of prior business records relating to an individual, and database services used primarily for risk assessment, lie outside the scope of the principles.

Increased market demand, a highly mobile society, as well as rapid advances in technology, have spurred increased reliance upon and availability of information obtained through services provided by companies in the individual reference services industry,

This increased reliance upon and availability of information has heightened consumer interest regarding privacy and identity fraud concerns, as well as services provided by companies within the individual reference services industry. It is notable that there is no evidence these services are used for unlawful purposes. Nor has any organization or study, including the Federal Reserve Board in its specially commissioned 1997 report to Congress, been able to point to a single case of identity fraud that resulted from the misuse of an individual reference service.

Members of the individual reference services industry recognize the importance of minimizing risks associated with their services, and are strongly committed to taking a leadership role on these issues. The IRSG also realizes that self-regulation of this industry is the most effective and efficient way to minimize these risks. It is with this background that the IRSG has adopted these principles.

SUMMARY OF PRINCIPLES:

IRSG members commit to educating their users and the public about the services they offer and the privacy issues that are associated with these services. An educational initiative will allow users and the public to understand the capabilities of these services, and enable users to utilize the information obtained from these services responsibly.

The principles mandate that companies in the individual reference services industry acquire individually identifiable information only from sources known as reputable in the government and private sectors. They also adopt the Direct Marketing Association's long-standing prohibition on the use for non-marketing purposes of personally identifiable information obtained from marketing transactions. This refers primarily to customer lists and other material that reflects transactions undertaken by an individual. Here, with a few exceptions, the principles prohibit services from knowingly purchasing or selling individually identifiable information that is collected for marketing purposes and from knowingly retaining such marketing information for inclusion in their individual reference services. This would include information obtained from customer lists, warranty card responses, and the like, While marketing data generally may not be used as an individual reference resource, individual reference services may be used for direct marketing purposes, such as verifying the addresses of individuals for delivery purposes,

The core of the IRSG's self-regulatory effort is the self-imposed restriction on use and dissemination of non-public information about individuals in their personal (not business) capacity In addition, IRSG members who supply non-public information to other individual reference services will provide such information only to companies that adopt or comply with the principles. The principles define the measures that IRSG members will take to protect against the misuse of this type of information, The restrictions on the use of non-public information are based on three possible types of distribution that the services provide.

For *selective and limited distribution* of non-public information, the companies commit to state what uses of their information are appropriate and to provide such products only to qualified subscribers. Such subscribers are required to state their appropriate purpose for using such information and agree to limit the use and redissemination of such information to those stated purposes. The subscribers' qualifications and intended uses will be reviewed before the non-public information is made available, with the extent and nature of the review determined by the nature of the non-public information being requested,

For *commercial and professional distribution* of non-public information, the companies commit to limiting distribution to established professional and commercial users who will use the information only for appropriate purposes within the normal course and scope of their business or profession. Certain categories of non-public information, such as financial or medical records, will be excluded from this type of distribution. Records that reveal an individual's mother's maiden name identified as such also will not be distributed. Social security numbers and date of birth information will be distributed only if truncated in an appropriate manner. For example, recognizing the importance of preventing the reconstruction of original information otherwise

protected by these principles, the industry has adopted the consistent practice of masking the last four or more digits of social security numbers. These exclusions are intended solely for non-public information, and will not apply to public or publicly available information that may contain social security numbers or similar data.

In order to protect against abuse in both *selective and limited distribution* and *commercial and professional distribution,* individual reference services will maintain certain records, including the identity of subscribers and the terms and conditions agreed to by them, for three years after termination of each subscriber's relationship with the individual reference service, In addition, the companies will take steps to remedy abuses, if any, that they may learn about.

For *general distribution* of non-public information, the companies will not knowingly provide non-public information products that contain an individual's social security number, mother's maiden name identified as such, non-published telephone directory information obtained from a phone company (as defined by Newton's Telecommunications Dictionary), date of birth information, credit history, financial history, medical records, or similar information. The services also will not provide products in which information is retrievable by input of a social security number. The individual reference service will take reasonable steps to protect against the misuse of non-public information provided in this type of distribution.

In addition to limiting access to non-public information, the principles require individual reference services to provide security to avoid unauthorized access to their materials, The security provided will include both technical and managerial controls to protect information. Periodic reviews of security also will be made to ensure the proper protection of information.

In the spirit of openness, the principles require individual reference services to have an information practices policy statement available to the public upon request. These statements will describe the types of information included, the types of sources from which that information is obtained, the nature of how the information is collected, the type of entities to whom the information may be disclosed, and the type of uses to which the information may be put. This openness will enable individuals to understand the reference service's use of the information it possesses.

Individual reference services will also inform individuals, upon request, of the choices, if any, available to limit access or use of information about them contained in the products and services that the companies create, maintain, or provide access to. The ability of an individual to limit access to his or her information should not serve as an impediment to law enforcement use of the databases. However, individual reference services will provide individuals with an opportunity to limit the public's access or use of non-public information about them that is distributed to the general public under principle V.C.

The principles also require an individual reference service to provide information about the nature of public record and publicly available information that it makes available in its products and services and the sources of such information. Subject to limited legal and security exceptions,

the companies will make available to individuals, upon request and under reasonable conditions, non-public information contained in products or services that specifically identifies them and that is distributed as part of an individual reference service to users.

The FTC disagrees with the IRSG's approach to responding to requests by individuals for public record information about themselves contained in a company's databases, Where the requested information is publicly available or a matter of public record, the principles allow the individual reference service to provide guidance on how the requester can obtain the information directly from the source. The FTC proposes that companies furnish individuals with all public record and publicly available information about themselves contained in the companies' databases in order to address two accuracy-related issues: first, the possibility that errors might arise in the transmission of information from the source to the company's database; and second, the possibility that information about different individuals might be mistakenly linked in compilations about a single individual.

The signatories of these principles understand the public's interest in enabling individuals to verify that errors do not occur when public record and publicly available information is transmitted or compiled about them. However, technological advancements have eliminated the need for most companies to keystroke or otherwise manually input this type of information, thereby significantly reducing the possibility for error. This, the signatories believe, when coupled with quality assurance measures implemented by the industry, yields information that reliably reflects the data provided by the originating public record source,

Moreover, there is an enormous potential burden associated with retrieving and verifying relevant information from the large number of databases of public records. This contrasts with the modest burden associated with retrieving information about an individual from the far smaller number of databases of non-public information. It should also be noted that many of the potential harms that might befall an individual whose public record information is inaccurate are already addressed by existing laws, including the Fair Credit Reporting Act.

Nevertheless, the signatories have pledged to reexamine, in 18 months, the issue of responding to requests by individuals for public record information about themselves.

In addition, the experience of applying these principles and conducting the assurance reviews will shed further light on the accuracy issue to the extent to which any inaccuracies might be derived from transmission or compilation errors that may occur under the control of an individual reference service. Based upon this experience, the signatories over the next 18 months will collectively or individually carefully consider undertaking a study to assess the accuracy of information about individuals in their databases as a reflection of the information about such individuals provided by the originating public record source.

In connection with children, the individual reference services industry recognizes the heightened sensitivity necessary in dealing with the individually identifiable information about

children. For this reason, the principles strictly limit the availability of non-public information concerning anyone identified as being under the age of eighteen.

The signatories of these principles commit to having annual assurance reviews conducted of those services they offer that they identify as being subject to the principles. These reviews will - be conducted by qualified independent professional services such as accounting firms, law firms, or security consultants. These independent professional services will use criteria developed by assurance professionals and approved by the signers as a group, As experience and changing circumstances require changes in the principles or in the criteria used for assurance reviews, the approval of the signers as a group will be needed to adopt such changes,

Companies will have a reasonable opportunity, determined by the nature of the concern and circumstances that surround it, to respond to any concerns that are expressed in such assurance reviews. Because individual reference services that obtain non-public information from IRSG members will be required by contract to abide by the principles, they, too, will need to have assurance reviews conducted annually.

While a summary of each assurance report shall be made publicly available, the signatories of these principles are exploring additional means of enabling the public to identify individual reference services that are in compliance with these principles.

The IRSG members believe that these principles provide the most effective way to secure the benefits of these important information service resources while assuring effective protection of consumer privacy, IRSG members pledge to implement these principles fully by no later than December 31, 1998.