

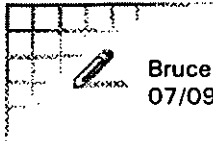
**NLWJC - Kagan**

**DPC - Box 008 - Folder 012**

**Consumer Safety - Right to Privacy**

**[1]**

*Cous pro-right to privacy*



Bruce N. Reed  
07/09/98 11:36:28 AM

Record Type: Record

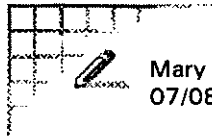
To: Mary L. Smith/OPD/EOP

cc: Thomas L. Freedman/OPD/EOP, Elena Kagan/OPD/EOP, Laura Emmett/WHO/EOP

Subject: Re: Privacy memo

Thanks. I think the 4 policy options are snoozers, but the legislative ideas sound more interesting.

Case pro-right to privacy



Mary L. Smith  
07/08/98 11:06:38 AM

Record Type: Record

To: Thomas L. Freedman/OPD/EOP, Bruce N. Reed/OPD/EOP, Elena Kagan/OPD/EOP  
cc: Laura Emmett/WHO/EOP  
Subject: Privacy memo

There is a deputies meeting on privacy today at 1 p.m. in Room 180. Below is the longer memo. I have also faxed it over to you. Here is the prepared summary of the topics to be discussed:

### Summary of policy options

1. **Privacy entity:** Designate a White House policy council or OMB to increase coordination on privacy issues.
2. **Online privacy:** Continue to press for industry self-regulation - with the option for a legislative solution if self-regulation proves to be inadequate.
3. **Privacy dialogue with state and local governments:** Initiate a "privacy dialogue" with state and local governments about the privacy of personal information collected by governments. Discussion could include: state privacy laws, use of Social Security numbers, impact of new technology on definition of "public records."
4. **Public education:** Work with the private sector and non-profits to develop an advertising campaign to inform individuals about how to exercise choice with respect to the collection and dissemination of their personally identifiable information.

### **Areas of particular sensitivity**

1. **Information about children:** Call for legislation that would specify a set of fair information principles applicable to the collection of data from children (e.g. no collection of data from children under 13 without prior parental consent).
2. **Medical records:** Call for legislation on privacy of medical records consistent with HHS report.
3. **Financial records:**
  - Call for amendments to Fair Credit Reporting Act to limit the "affiliate sharing exception." Businesses could share consumer information for marketing purposes, but not for business decisions. For example, consumer information

provided to an insurance affiliate could not be used to deny a person a loan without FCRA protection.

- Authorize the Fed to write enforceable rules on inter-affiliate information sharing.
  - Determine whether Justice and FTC have adequate jurisdiction and penalties to punish theft of personal financial information.
4. **Profiling:** Call for legislation that would give the FTC the authority to require “profilers” to comply with a set of fair information practices. Profilers are in the business of compiling and distributing electronic dossiers on individually identifiable consumers.
5. **Identity theft**
- Endorse Kyl bill on identity theft, provided it addresses concerns of Treasury and Justice.
6. **Social Security Numbers:** Conduct a study that looks backward to discern “lessons learned” from social security experience and looks forward to avoid the same result with respect to new identification technologies (e.g. biometrics).

----- Forwarded by Mary L. Smith/OPD/EOP on 07/08/98 11:06 AM -----



**Thomas A. Kalil**

07/08/98 10:49:31 AM



Record Type: Record

To: Mary L. Smith/OPD/EOP

cc:

Subject: Privacy memo



.... PRIVACY.J

It's at 1 p.m. in Room 180. Attached is a cover memo plus more detailed memo from Commerce.

----- Forwarded by Thomas A. Kalil/OPD/EOP on 07/08/98 10:52 AM -----

*Cons pro-right to privacy*

THE WHITE HOUSE  
WASHINGTON

July 7, 1998

MEMORANDUM FOR NEC/DPC DEPUTIES

FROM: Sally Katzen, Tom Kalil  
RE: July 8th Deputies meeting on privacy

Attached is a paper on a set of policy options to address privacy issues that has been prepared by the NEC/DPC Working Group on Privacy. This package is designed to:

- Address "cross-cutting" issues that affect a range of privacy concerns (privacy entity, privacy online, dialogue with state and local government, and public education);
- Target sectors or users that are particularly sensitive (children, medical records, financial records, profiling, identity theft, social security numbers);
- Address both "offline" and "online" privacy;
- Encourage self-regulation where possible and identify the need for legislation where necessary; and
- Maintain a balanced approach that recognizes the values associated with the free flow of information and with giving individuals greater control over their personally identifiable information.

We would like to use the meeting tomorrow to determine where we have consensus and where there may be areas of disagreement. It is our intent to schedule a Principals meeting on privacy as soon as possible.

Summary of policy options

**Cross-cutting**

1. **Privacy entity:** Designate a White House policy council or OMB to increase coordination on privacy issues.
2. **Online privacy:** Continue to press for industry self-regulation - with the option for a legislative solution if self-regulation proves to be inadequate.

3. **Privacy dialogue with state and local governments:** Initiate a "privacy dialogue" with state and local governments about the privacy of personal information collected by governments. Discussion could include: state privacy laws, use of Social Security numbers, impact of new technology on definition of "public records."
4. **Public education:** Work with the private sector and non-profits to develop an advertising campaign to inform individuals about how to exercise choice with respect to the collection and dissemination of their personally identifiable information.

#### **Areas of particular sensitivity**

1. **Information about children:** Call for legislation that would specify a set of fair information principles applicable to the collection of data from children (e.g. no collection of data from children under 13 without prior parental consent).
2. **Medical records:** Call for legislation on privacy of medical records consistent with HHS report.
3. **Financial records:**
  - Call for amendments to Fair Credit Reporting Act to limit the "affiliate sharing exception." Businesses could share consumer information for marketing purposes, but not for business decisions. For example, consumer information provided to an insurance affiliate could not be used to deny a person a loan without FCRA protection.
  - Authorize the Fed to write enforceable rules on inter-affiliate information sharing.
  - Determine whether Justice and FTC have adequate jurisdiction and penalties to punish theft of personal financial information.
4. **Profiling:** Call for legislation that would give the FTC the authority to require "profilers" to comply with a set of fair information practices. Profilers are in the business of compiling and distributing electronic dossiers on individually identifiable consumers.
5. **Identity theft**
  - Endorse Kyl bill on identity theft, provided it addresses concerns of Treasury and Justice.
6. **Social Security Numbers:** Conduct a study that looks backward to discern "lessons learned" from social security experience and looks forward to avoid the same result with respect to new identification technologies (e.g. biometrics).

*Cons pro-right to privacy*

**MEMORANDUM**

**TO:** Sally Katzen  
**FROM:** Andrew Pincus  
**DATE:** July 7, 1998  
**RE:** Privacy – Legislative and Other Options

This memorandum outlines a series of Administration proposals for enhancing privacy protection by acting in the following areas:

- Creation of a Federal Privacy Entity
- Medical Records
- Profiling
- On-line Information About Children
- Government Information
- Credit Reporting
- Financial Industry
- Identity Theft
- Theft of Personal Information
- Public Education
- Social Security Numbers
- Commercial Marketing

### CREATION OF A FEDERAL PRIVACY ENTITY

New technologies have made it easier to create, manipulate, store, transmit, and link digital personally identifiable information. Many Americans believe that they have lost all control over how personal information about them is circulated and used by companies. We can expect that these issues will become more important and prominent with the advent of new technologies such as the Internet, electronic commerce, and data mining.

Privacy concerns often, however, have to be accommodated with competing values - such as prevention of crime, prosecution of criminals, cracking down on "deadbeat parents," free expression, an investigatory press, and the economic and commercial benefits that come from the free flow of information.

Attempting to centralize privacy policy development within the Administration would not make any sense. Inevitably, many agencies will have to deal with some aspect of privacy policy - Education on student records, HHS on medical records, Transportation on Intelligent Transportation Systems, etc.

There is, however, an increased need for coordination across agency lines, precisely because privacy is a cross-cutting issue. This would be particularly helpful in the following four areas:

- *Representational* - Better explain and promote the Administration's privacy policy domestically and internationally. Currently, the United States is not represented in many important international fora on privacy.
- *Consumer Information* - Increase public awareness of privacy issues and the rights and responsibilities of consumers, industry, and government. Use the "bully pulpit" to encourage best practices and criticize bad actors.
- *Advisory* - Provide/coordinate advice on privacy policy questions to government agencies and the private sector.
- *Coordination* - Ensure that agencies are addressing emerging privacy issues, and ensure greater consistency of Administration positions and policies.

#### Option

The Administration could create a Federal privacy entity located in the Executive Office of the President.

There are advantages and disadvantages to putting it in OMB, making it a new White House office, or putting it under one of the existing White House policy councils. Since shaping privacy policy requires accommodating different interests, it would be better if it were located in



an office that had other responsibilities. Having an office that saw itself *exclusively* as a "privacy advocate" would be counter-productive.

The entity should have a small staff — since the intent is to have it play a coordinating role as opposed to an operational role.

### HEALTH INFORMATION

The confidentiality of health information is a matter of widespread national concern, and the protection of this information has been a priority of the Administration. On September 11, 1997, Secretary of Health and Human Services Donna Shalala recommended that Congress enact Federal legislation to protect the confidentiality of health information by imposing duties on those who hold such information and providing rights to the subjects of the information. She proposed that the Federal law provide a floor of protection, and that States be permitted to, in addition, provide stronger protections.

Under the recommended legislation, health care providers, those who pay for health care, and those who get information from those entities would have to permit patients to see their own records, to keep records of disclosures and let patients know who has seen their records, and to permit patients to file proposals for correction of erroneous records. All entities collecting or maintaining information would have to advise patients clearly of their confidentiality practices and of the patients' rights.

Disclosures would be limited to those authorized by the patient, or those specifically permitted in the legislation, including disclosures for important public purposes, such as treatment and payment, research, public health, oversight of the health care system, and use in law enforcement or other legal proceedings if permitted by other law. There would be strict limitations on further disclosure in many of these instances. Within an organization, information could be used only for purposes reasonably related to the purposes for which it was gathered, and all disclosures would have to be limited to the minimum necessary to accomplish the purpose of the disclosure.

Entities receiving information pursuant to patient authorization would have to give patients a statement of their intended use of the information, and would be civilly liable for uses in violation of that statement.

There would be civil and criminal sanctions for violations, such as improper disclosure and obtaining information under false pretenses.

Congress is now considering the recommendations.

## PROFILING

Commercial "profilers" build dossiers about individuals by aggregating information from a variety of database sources, including public and non-public records. Individual reference services, sometimes called look-up services, represent a sub-set of the profiling industry. These services provide information that assists users in identifying individuals, locating individuals, and verifying identities.

### Best Practices Model - Individual Reference Services Group

On December 17, 1997, a group of 14 Individual Reference Services (the Individual Reference Services Group, IRSG) entered into an agreement on privacy practices with the Federal Trade Commission. The IRSG program is based on compliance with certain principles, including notice, disclosure, choice, security, and public education. IRSG members agreed to acquire personal information only from reputable sources, to take reasonable steps to assure that data collected is accurate, complete and timely for the purpose for which it will be used, to correct non-public records when appropriate, and to limit distribution of non-public information to subscribers with appropriate intended uses.

The IRSG committed to implement a rigorous enforcement compliance method. The enforcement program has two prongs. First, signatories' practices are subject to review by a "reasonably qualified independent professional service." On the basis of established criteria, that entity determines whether a signatory is in compliance with IRSG principles. The results of the annual review are made public. Second, signatories who are information suppliers may not sell information to look-up services that do not comply with the IRSG principles.

The IRSG members agreed to provide individuals with access to information contained in services and products that specifically identify them, unless the information comes from a public record, in which case the companies will provide the individuals with guidance on how they can obtain the information from the original source. FTC staff strongly disagreed with the access provisions of the IRSG practices, and the Commission and IRSG agreed to allow 18 months before revisiting the access issue. On the basis of the IRSG program and the commitment to review access issues, the FTC advised the Congress that legislation on individual reference services was premature.

### Legislative Option

The Administration could embrace the IRSG approach and apply it more broadly by supporting legislation giving the FTC authority under Section 5 of the FTC Act to require those in the business of compiling and distributing (or re-using for marketing purposes) electronic dossiers on individually identifiable consumers to comply with a specified set of fair information practices. The grant of authority to the FTC could include a "safe harbor" provision -- profilers

who belong to a self-regulatory organization operating in accordance with practices approved by the FTC would be presumed to be in compliance with the Federal Trade Commission Act.

### ON-LINE INFORMATION ABOUT CHILDREN

The solicitation of information from children presents a unique problem. Unlike adults, children generally lack the ability to provide legally binding consent and may not be cognitively capable of understanding the consequences of giving out personally identifiable information online. Many companies presently collect information from children for a variety of reasons – to contact a child to verify that they may have won a prize, to monitor children in chat rooms, for statistical purposes or for direct marketing purposes.

On June 4, 1998, the Federal Trade Commission released a report to Congress, *Privacy Online*, which surveyed 1,400 Web sites. Eighty-nine percent of children's sites surveyed collect personal information from children. Although 54% of children's sites provide some form of disclosure of their information practices, the Commission found that few sites take any steps to provide for meaningful parental involvement in the process. They found that only 23% of sites even direct children to seek parental permission before providing personal information. Only 7% of the sites said they would notify parents of their information practices, and less than 10 % provide for parental control over the collection and/or use of information from children. The Commission recommended that Congress adopt legislation protecting children's privacy online.

#### Best Practices Model – Online Privacy Alliance

On June 22, 1998 the Online Privacy Alliance issued specific guidelines for the protection of children's' privacy online.

Alliance members that operate sites directed at children under 13 have agreed (1) not to collect online contact information from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of this information, including an option for the parent to prevent the use of the information and participation in the activity; (2) to assure that information collected will only be used to directly respond to the child's request and will not be used to recontact the child for other purposes without prior parental consent; (3) not to collect individually identifiable offline contact information from children under 13 without prior parental consent; (4) not to distribute to third parties any personally identifiable information collected from a child under 13 without prior parental consent; (5) not to give children under 13 the ability to post or otherwise distribute individually identifiable contact information without prior parental consent – sites directed to children under 13 must take best efforts to prohibit a child from posting contact information; and (6) not to entice a child under 13 by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in that activity.

### Legislative Option

The Administration has endorsed the FTC call for legislation with respect to children's privacy online. The Administration could call for legislation that would specify a set of fair information practices applicable to the collection of data from children and give the FTC authority to promulgate rules based on such standards. The grant of authority to the FTC could include a safe harbor provision – data collectors who belong to a self regulatory organization operating in accordance with practices approved by the FTC for the collection of data from children would be presumed to be in compliance with the Federal Trade Commission Act.

### RELEASE OF GOVERNMENT INFORMATION

Public records are a rich store of personal information. Federal, state and local governments require individuals to provide various types of information and are usually required to make such records available for public inspection. Public records include, but are not limited to real property records, marriage and divorce records, birth and death certificates, driving records, driver's licences, 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, worker's compensation claims, political contributions records, firearm permits, occupational and recreational licenses, filings pursuant to the Uniform Commercial Code and filings with the Securities and Exchange Commission.

These public records contain extensive and detailed information (e.g., race, gender, Social Security numbers, addresses, dates of birth, marriage, and divorce.) Social Security numbers, for example, are available from the records kept by dozens of government entities, such as motor vehicle bureaus – many driver's license records make the individual's SSN, as well as their name, address, height, weight, eye color, gender, and date of birth available in one place. Dates of birth may be available from birth certificate and voter registration records, and land records typically include dates of sales, prices, size of mortgage amounts, and the property address and description, as well as the seller's and purchaser's names.

The U.S. Privacy Act, 5 U.S.C. Section 552a (1988) protects individuals from non-consensual government disclosure of confidential information. The Memorandum for Heads of Executive Departments and Agencies, signed by the President on May 14, 1998, directs agency heads to take specific action to assure that use of new information technologies sustain privacy protections provided by applicable statutes and that the information is handled in full compliance with the Privacy Act.

While the U.S. Privacy Act restricts the disclosure of personal information collected and maintained by the Federal government, many States do not have analogous privacy laws. Not only is the protection of information collected and maintained by State governments governed by an uneven patchwork of laws, but State freedom of information and public record laws, enacted

before powerful information technology made collection and dissemination of information easy and efficient, allow many States to sell personal information.

Issues around the collection, sharing and sale of personal information gathered by States are complicated by requirements under Federal law that States collect and provide certain information to the Federal government. These laws include transfer of information for tax purposes, to locate parents delinquent in their child support payments, and to determine food stamp and welfare eligibility.

Any effort to restrict State collection and sharing of personal information will raise significant federalism questions. For example, two states have successfully challenged the Drivers Privacy Protection Act on federalism grounds.

The Administration has already begun to address the issue of sharing of data by Federal agencies with State, local, and tribal governments in the President's Memorandum to Heads of Executive Departments and Agencies, signed on May 14, 1998.

#### Option

The Administration could create a Federal-State Task Force to initiate a "privacy dialogue" to analyze the privacy of personal information collected by governments. The dialogue could include a study of the State laws that require the collection of personal information and the Federal laws that require States to collect personal information and consider the desirability of:

1. State enactment of laws similar to the Privacy Act.
2. Extension of the Privacy Act protections to Social Security numbers collected by State governments.
3. Re-evaluation of the meaning of "public records" in light of new technology.
4. A requirement that States redact Social Security numbers and other personally identifiable information from documents before they are placed in the public domain.
5. An Executive Memorandum to public schools reiterating obligations imposed by the Family Educational Rights and Privacy Act of 1974 under which public schools that accept federal funds are prohibited from disclosing a student's Social Security number and personal information without the student's request.
6. An Executive Memorandum to State attorneys general reiterating obligations imposed by §7 of the Privacy Act with regard to the protections afforded the collection of Social Security numbers and the requisite notice requirements.

## CREDIT REPORTING

The Fair Credit Reporting Act (FCRA) governs activities of agencies that furnish credit reports to third parties. The FCRA defines a credit reporting agency as a person or entity that regularly assembles or evaluates consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties to be used as a factor in establishing the consumer's eligibility for credits, insurance, employment purposes, etc.

Companies that share consumer information with their affiliates are not subject to the controls of the FCRA. Based on the above definitions, these companies are not considered "credit reporting agencies" because they are not providing the reports to a third party, but rather to themselves. Additionally, the information shared is not considered a "credit report" because the information is not compiled by a "credit reporting agency." The FCRA, moreover, specifically excludes affiliate sharing from the definition of "credit report."

The exclusion of affiliate sharing from the credit report definition and further regulation by the FCRA was debated during the 1996 Amendments to the FCRA. The FTC strongly argued that consumer information shared by affiliates should be subject to the protections of the FCRA. The banking industry argued the opposite. The banking industry won; the FCRA specifically excludes the information shared by affiliates from the definition of consumer report.

The recent increase in cross-industry corporate mergers raise important privacy concerns with regard to the treatment of consumer information shared by affiliated companies. Such mergers may allow detailed and sometimes sensitive information about consumers, including medical and financial data, to be shared among newly related companies with relatively few restrictions. In the case of the recent merger of Citicorp and Travelers, for example, consumers might not anticipate that providing information for insurance underwriting purposes to one entity might later be used by the financial institution that is or becomes an affiliate.

### Legislative Options

a. The Administration could call for legislation repealing the FCRA provisions that exempt affiliate sharing from the protections of the FCRA. Given the intensity of the debate on this issue during the negotiations over the 1996 Amendments and the banking industry's current opposition to this issue, this proposal may be extremely difficult to effectuate. The FTC would probably, however, support repeal of the affiliate sharing exemption.

b. The Administration could support amendments to the FCRA to limit the affiliate sharing exception for marketing purposes only and expand the protections of the FCRA to cover consumer information shared with affiliates when making business decisions. For example, businesses could share consumer information among affiliates in connection with a marketing campaign, but consumer information provided for insurance underwriting purposes to one entity could not be used by another entity to deny a person a loan without the protections of the FCRA.

implicated. This proposal may appease the banking industry, which uses the information mainly for marketing purposes, while still protecting the consumers. The FTC probably would support such action.

### Study Option

As more databases are available directly to companies, and companies themselves share information directly, there is some concern that the FCRA may become outdated and obsolete. Companies, for example, will no longer purchase credit reports from a central bureau, but rather will obtain information directly from the individual sources and create their own internal credit reports. In the absence of traditional credit reporting agencies, the protections of the FCRA would evaporate. The Administration could undertake a study to determine whether the FCRA contains the protections needed in the electronic age.

## FINANCIAL INDUSTRY

On June 12, 1998, the Acting Comptroller of the Currency announced that she directed the Office of the Comptroller of the Currency's (OCC) Privacy Working group to develop guidance for national banks addressing a number of consumer privacy issues, including web site disclosures of bank privacy policies, sharing of consumer information, customer information security and the problem of identity theft.

### *Sharing of Confidential Information with Third Parties (e.g. Direct Marketers)*

Financial services firms represent that they do not generally share confidential customer information with third parties (except service providers). Privacy advocates have not contradicted this assertion. Financial firms have three primary reasons for retaining this information: (1) the most likely purchasers of such information are the firm's competitors; (2) financial firms fear that their customers would react badly if they learned that their information was being sold; and (3) sale of such information is generally prohibited by State common law (i.e., the financial institution, acting as the agent of the customer, owes the customer a fiduciary duty and is prohibited from misusing information obtained from the customer in connection with the agency).

The NASD-R recently proposed a new confidentiality rule for securities firms.

In the area of direct marketing by the financial institution itself, the FCRA requires that customers of financial institutions be allowed to opt out of receiving pre-approved offers of credit cards or other credit. NASD and the FTC rules restrict the ability of securities brokers to cold call customers by, among other things, requiring the maintenance of "do-not-call" lists.

### Option

Conduct a study to determine exactly what the financial services industry's practices are in this area.

### *Sharing of Information with Affiliated Companies*

Each of the nations' largest 25 banks has a securities affiliate, and banks of all sizes sell insurance. Affiliate information sharing already includes not only sharing of information for marketing purposes (e.g., a credit card bank soliciting an affiliate broker-dealer's best customers for a new platinum card) but also for security purposes (e.g., tracking a credit card holder's spending patterns in order to detect immediately any unusual activity that might indicate fraud or theft) and increasingly for risk-management purposes (e.g., a customer's record of payment on a credit card apparently is quite useful in determining whether that customer is a good risk for auto insurance). Such practices can be expected to continue, as the lines between various types of financial services firms continue to blur and the firms continue to merge.

Under the 1996 Amendments to the FCRA, customers have an explicit right to opt out of affiliate information sharing of personal information other than "experience" or "transactional" information (which may be shared not only with affiliates but also third parties). For example, a customer can prevent personal information contained in an account application from being shared. As a result, customers can generally avoid use of their confidential information for marketing purposes but not for fraud prevention or risk management purposes. This limited right was also brokered as part of the 1996 Amendments to the FCRA.

The FCRA also contains an odd provision prohibiting the banking agencies from examining for compliance with the Act; rather, they must await a complaint or other indication of trouble. The banking regulatory agencies also are prevented from issuing regulations under the Act, but the Federal Reserve may promulgate "interpretative" opinions in consultation with the other agencies. These provisions were included in 1996 because of banking industry concerns about regulatory burden, as part of the delicate compromise that moved the bill forward.

The Fed expects to issue an interpretation sometime this summer which likely would clarify what information can be shared with affiliates and how specific opt out notices should be.

### Options

a. Authorize the Fed, in consultation with the other banking agencies, to write enforceable rules in this area. Alternatively, give this authority to each of the agencies, to be exercised jointly.



b. Consider eliminating the restriction on examinations. We may wish to talk to privacy groups next week to see whether this step, which would certainly anger the banking industry, would achieve greater protection for consumers.

*Note:* Consultations with those on the Hill should precede any action in this area, as they may not wish to revisit the compromise that it took them years to reach in 1996.

#### Study Option

The Administration could review whether the regulatory review process for mergers should include a consumer protection analysis. For example, in addition to Justice Department review of a proposed commercial merger, the regulating agency could review the proposed merger to determine whether the merger negatively affects consumers' privacy.

#### *On-Line Disclosures*

Large banks generally have adopted the privacy principles promulgated by the banking trade groups and have posted these or similar privacy policies on their web sites, while smaller banks have been slower to do so.

The Comptroller of the Currency has announced that it will consider promulgating voluntary guidelines for national banks to use in constructing web sites, and the FDIC's E-banking Task Force is surveying web sites of FDIC-insured institutions to confirm, based on a larger survey group, whether the results of the FTC survey accurately reflects the practices of the nation's smaller state banks.

Main Treasury met with each of the federal banking agencies (OCC, FDIC, Fed, and OTS) to discuss parallel action in the privacy area by all regulators. Each banking agency has accorded a high priority to the privacy issue and is looking at possible areas for strengthening regulatory practices and encouraging improved policies and procedures by regulated institutions. The banking agencies agreed to coordinate informally their previously independent efforts at establishing guidelines and examiner guidance with respect to banking industry on-line privacy disclosures.

#### Option

The Administration could officially encourage continued consultative efforts, while recommending more formal coordination efforts.

## IDENTITY THEFT

The term "identity theft" generally refers to the fraudulent use of another person's identity to facilitate the commission of a crime, such as credit card fraud. To commit identity fraud, a criminal gathers information about a person and then uses the information to adopt the identity of a victim.

Under existing law, identity theft offenses are punished to the extent that they include identification documents (i.e., forged or stolen documents) and an intent to defraud the United States. Yet existing law does not reach identity theft that makes use of other means of identification, such as a social security number or a mother's maiden name.

For this reason, it would be helpful to change the law to recognize the potential harm that could be done by offenders who commit identity theft with means of identification, and to address other problems that have emerged as a result of a dramatic increase in cases of identity theft.

At the same time, legislation to criminalize identity theft must be carefully crafted to avoid problems that could arise from the federalization of a large new class of crimes.

Senator Kyl is in the process of marking up S. 512, the Identity Theft and Assumption Deterrence Act of 1997. After raising initial technical concerns about this bill, Departments of Treasury and Justice have worked to provide amendments (to be considered during markup) that would address any outstanding concerns.

### Legislative Options

a. The Administration could endorse the Kyl bill and work with him toward passage, provided that the reported version adequately address concerns of the Treasury and Justice Departments.

b. Merchants require check-writers to provide proper identification, which often includes a driver's license or other identification card with a social security number. Usually a merchant will record the identifying number onto the check to provide proof of the verification activity. This simple action can create a realm of problems. As a result of this activity, a person's check, which contains a person's name, address, and bank account number, now also contains the individual's social security number. By linking these pieces of personal information together on a single check a merchant has made this customer an even better target for identity theft.

The Administration could seek legislation that makes it illegal to record social security numbers on a check that is being approved for a purchase. This would mirror a law that was passed several years ago that prohibited the recording of a credit card number onto a check when the credit card was used as a piece of identification. Such legislation would neither make it

illegal for a merchant to ask for the identification, nor indicate that such a check occurred. The law would merely prohibit writing the actual social security number on the check. Note, however, that modern "telecheck" technology permits merchants to ensure that a personal check is good without a Social Security number.

### **THEFT OF PERSONAL INFORMATION**

In this case, which is the mirror image of identity theft, the offender obtains information illegally but then uses it for a legal purpose – e.g., pretends to be a customer in order to trick confidential information out of a bank, and then sells that information to a private investigator, perhaps in a divorce case.

Chairman Leach has publicized this problem and is strongly committed to correcting it. His staff, however, is having a difficult time trying to do so. They have apparently abandoned imposing greater restrictions on bank security or greater criminal penalties on those who obtain the information. We had suggested that they speak to the FTC about whether civil enforcement was a possibility.

#### **Recommendation**

The Administration could explore whether the FTC and DOJ have adequate jurisdiction or penalties to punish those who obtain information by fraudulent means.

*Note:* There may be a problem of unclean hands here, as law enforcement is a primary consumer of this information.

### **PUBLIC EDUCATION**

The U.S. approach to privacy focuses on choice – individuals should have the choice to protect or disclose most personal information. Many Americans are unaware of how their personal information is used, and they do not understand how to protect themselves or exercise their ability to choose. Likewise, many businesses are unaware of consumer concerns about privacy and have not thought through their information handling practices in light of this concern.

The Administration could identify private sector partners to develop an advertising campaign to inform individuals about how to exercise choice with respect to the collection and dissemination of their personally identifiable information. Such a campaign could include all advertising mediums – radio, television, print, and electronic.

Cons pro -  
RT privacy

## MEMORANDUM

TO: Sally Katzen  
FROM: Andrew Pincus  
DATE: July 16, 1998  
RE: Privacy - Legislative and Other Proposals

This memorandum outlines a series of Administration proposals for enhancing privacy protection by acting in the following areas:

- Federal Privacy Coordination Responsibility
- On-Line Collection of Information Generally (Commercial Marketing)
- On-Line Collection of Information from Children
- Government Information
- Medical Records
- Financial Records
- Profiling
- Identity Theft/Theft of Personal Information
- Protection of New Categories of Personal Information
- Public Education

These initiatives would follow-up on those announced by the Vice President on May 14, 1998 in his speech at New York University.

## FEDERAL PRIVACY COORDINATION RESPONSIBILITY

Concerns about privacy are shared across agencies. Some privacy activities are undertaken by many; others by no one. Early in the Administration, the President's Information Infrastructure Task Force (IITF) solicited and received public comments on whether there should be an entity within the executive branch to serve as a focal point for public and private sector privacy issues. The IITF reached no conclusion. This proposal concludes that work and responds in part to the July 1997 Presidential direction to develop recommendations as to the appropriate role of government in privacy.

### Proposal

The President could assign coordination responsibility of privacy issues to the Administrator of the Office of Information and Regulatory Affairs (OIRA) of OMB. This assignment would strengthen the ability of the Administration to develop and implement effective privacy policy.

OMB recognizes that many agencies have expertise and responsibility for privacy in various areas, however, additional focus on privacy across the executive branch would be useful. This increased focus would be accomplished by the performance of four functions by OMB:

- *Coordination* - Assure that agencies address emerging privacy issues in their programs and policies, and promote greater consistency of Administration positions and policies.
- *Advice* - Drawing on agency expertise, provide advice on privacy policy questions to government agencies and the private sector.
- *Representation* - Explain and promote the Administration's privacy policy domestically and internationally.
- *Consumer Information* - Increase public awareness of privacy issues and the rights and responsibilities of consumers, industry, and government. Use the "bully pulpit" to encourage best practices and criticize bad actors.

Rather than create a new privacy office or entity, it is more appropriate to assign these functions to the Administrator of OIRA. Privacy concerns must usually be balanced with competing values, such as prosecution of criminals, identifying "deadbeat" parents, free speech, and the economic and commercial benefits that come from the free flow of information. OMB is the traditional coordinator of policy, regulatory and organizational issues, while OIRA is already responsible for other information policy matters and has expertise and authority in privacy under the Privacy Act. OIRA, therefore, is a logical place to assign the new responsibilities. To be an effective coordinator, additional resources would be required, however, minimal resources are necessary since the proposed role is primarily coordination, not operations.

## ONLINE COLLECTION OF INFORMATION

Protection of privacy in the online environment was addressed in the *Framework for Global Electronic Commerce* released by the President on July 1, 1997. In that document, the Administration reaffirmed the importance of "assur[ing] personal privacy in the networked environment" and endorsed the Privacy Principles adopted in June 1995. The Administration "support[ed] private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes." It cautioned that "[i]f privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online."

In the year since the issuance of the *Framework*, the privacy issue has garnered significant public attention. The Administration has undertaken broad outreach efforts to urge industry to take up the challenge of self-regulation. Numerous media stories have addressed the threat to privacy in the online environment. And the Federal Trade Commission's net survey demonstrated that -- as of March 1998 -- online enterprises were devoting insufficient attention to privacy concerns.

At the same time, there has been significant progress on industry self-regulation. On June 22, 1998 a group of 50 businesses and trade associations announced the formation of the Online Privacy Alliance. The Alliance adopted well-received guidelines for fair information practices applicable across a range of industries, including the marketing industry. The Direct Marketing Association, which represents over 3700 direct marketers, has endorsed the Alliance guidelines, and committed to require DMA members to comply with the guidelines as a condition of membership in the association.

The Alliance guidelines require members to adopt and implement a policy for protecting the privacy of individually identifiable information. An organization's privacy policy must be easy to find and understand and must state clearly what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information, as well as the consequences, if any, of an individual's refusal to provide information. The policy should also include a clear statement of the organization's accountability mechanism and information about how to contact the organization if a problem or complaint arises. At a minimum, individuals should be given the opportunity to opt out of uses that are unrelated to the purpose for which the information was collected. The Alliance guidelines also require data collectors to take appropriate steps to ensure the security, reliability and accuracy of personally identifiable information.

The Direct Marketing Association has imposed additional requirements specific to marketing activities. These include a mandatory participation in the "Telephone Preference Service" and the "Mail Preference Service" through which consumers can have their names placed on a national "do not solicit" list.

The Alliance has committed itself to announce its approach to enforcement -- the final element of its privacy protection program -- within the next ten days. Based on our understanding of the likely ingredients of the enforcement approach, we believe the Alliance plan will satisfy the Administration's privacy principles. The Alliance's membership constitutes between 80 and 90 percent of online traffic.

In addition, the Council of Better Business Bureaus (CBBB) announced on June 22, 1998, that it will develop and implement a major privacy program through its subsidiary, BBBOnline. According to the CBBB press release, the online privacy program will feature: privacy standard-setting, verification, monitoring and review, consumer dispute resolution, compliance "seal", and educational components. The program is expected to "go live" in the fourth quarter of 1998.

TRUSTe is a not-for-profit organization based in the Silicon Valley. The TRUSTe program provides notice by Web sites of their information practices, verification and oversight of the claims made in the site's notice, and consumer recourse through which consumer complaints will be resolved. TRUSTe has been criticized for its failure to require adherence to fair information practices -- any practice is permitted, as long as it is disclosed. On June 24, 1998, however, TRUSTe announced that it would require all new and renewing licensees to adhere to the privacy guidelines announced by the Online Privacy Alliance.

### Proposal

The Administration should commend the members of the Online Privacy Alliance and other groups for the progress on self-regulation. We should, however, make clear that substantial challenges lie ahead. First, the privacy protections promised by these organizations must be redeemed -- these new organizations must become functioning entities. Second, the private sector must work to expand membership in self-regulatory organizations so that privacy protection becomes ubiquitous in the online environment. Obviously the Administration will also play an important role in this effort. We should repeat the caveat in the *Framework* that the absence of continued real progress will cause the Administration to reexamine whether government must take a more direct role in privacy protection.

OK, I guess

### ON-LINE INFORMATION ABOUT CHILDREN

The solicitation of information from children presents a unique problem. Unlike adults, children generally lack the ability to provide legally binding consent and may not be cognitively capable of understanding the consequences of giving out personally identifiable information online. Many companies presently collect information from children for a variety of reasons -- to contact a child to verify that they may have won a prize, to monitor children in chat rooms, for statistical purposes or for direct marketing purposes.

On June 4, 1998, the Federal Trade Commission released a report to Congress, *Privacy Online*, which surveyed 1,400 Web sites. Eighty-nine percent of children's sites surveyed collect personal information from children. Although 54% of children's sites provide some form of disclosure of their information practices, the Commission found that few sites take any steps to provide for meaningful parental involvement in the process. They found that only 23% of sites even direct children to seek parental permission before providing personal information. Only 7% of the sites said they would notify parents of their information practices, and less than 10 % provide for parental control over the collection and/or use of information from children. The Commission recommended that Congress adopt legislation protecting children's privacy online.

#### Best Practices Model – Online Privacy Alliance

On June 22, 1998 the Online Privacy Alliance issued specific guidelines for the protection of children's' privacy online.

Alliance members that operate sites directed at children under 13 have agreed (1) not to collect online contact information from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of this information, including an option for the parent to prevent the use of the information and participation in the activity; (2) to assure that information collected will only be used to directly respond to the child's request and will not be used to recontact the child for other purposes without prior parental consent; (3) not to collect individually identifiable offline contact information from children under 13 without prior parental consent; (4) not to distribute to third parties any personally identifiable information collected from a child under 13 without prior parental consent; (5) not to give children under 13 the ability to post or otherwise distribute individually identifiable contact information without prior parental consent – sites directed to children under 13 must take best efforts to prohibit a child from posting contact information; and (6) not to entice a child under 13 by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in that activity.

#### Proposal

The Administration already has endorsed the FTC's call for legislation with respect to protection of children's privacy in the online environment. The Administration should specify that this legislation should set forth the fair information practices applicable to the collection of information from children and grant the FTC authority to promulgate rules to implement these standards. The grant of authority to the FTC could include a safe harbor provision -- data collectors that belong to a self-regulatory organization that contains standards for collection of data from children acceptable to the FTC would be presumed to be in compliance with the statutory requirement and would not be subject to direct enforcement action by the FTC.

OK



## GOVERNMENT INFORMATION

Public records are a rich store of personal information. Federal, state and local governments require individuals to provide various types of information and are usually required to make such records available for public inspection. Public records include, but are not limited to real property records, marriage and divorce records, birth and death certificates, driving records, driver's licences, 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, worker's compensation claims, political contributions records, firearm permits, occupational and recreational licenses, filings pursuant to the Uniform Commercial Code and filings with the Securities and Exchange Commission.

These public records contain extensive and detailed information (e.g., race, gender, Social Security numbers, addresses, dates of birth, marriage, and divorce.) Social Security numbers, for example, are available from the records kept by dozens of government entities, such as motor vehicle bureaus -- many driver's license records make the individual's SSN, as well as their name, address, height, weight, eye color, gender, and date of birth available in one place. Dates of birth may be available from birth certificate and voter registration records, and land records typically include dates of sales, prices, size of mortgage amounts, and the property address and description, as well as the seller's and purchaser's names.

The U.S. Privacy Act, 5 U.S.C. Section 552a (1988) protects individuals from non-consensual government disclosure of confidential information. The Memorandum for Heads of Executive Departments and Agencies, signed by the President on May 14, 1998, directs agency heads to take specific action to assure that use of new information technologies sustain privacy protections provided by applicable statutes and that the information is handled in full compliance with the Privacy Act.

While the U.S. Privacy Act restricts the disclosure of personal information collected and maintained by the Federal government, many States do not have analogous privacy laws. Not only is the protection of information collected and maintained by State governments governed by an uneven patchwork of laws, but State freedom of information and public record laws, enacted before powerful information technology made collection and dissemination of information easy and efficient, allow many States to sell personal information. State records are the source of much of the personal information that, when disseminated, generates the greatest concern about privacy protection.

Issues around the collection, sharing and sale of personal information gathered by States are complicated by requirements under Federal law that States collect and provide certain information to the Federal government. These laws include transfer of information for tax purposes, to locate parents delinquent in their child support payments, and to determine food stamp and welfare eligibility.

Any effort to restrict State collection and sharing of personal information will raise significant federalism questions. For example, two states have successfully challenged the Drivers Privacy Protection Act on federalism grounds.

The Administration has already begun to address the issue of sharing of data by Federal agencies with State, local, and tribal governments in the President's Memorandum to Heads of Executive Departments and Agencies, signed on May 14, 1998.

### Proposal

The Administration should create a Federal-State Task Force to initiate a "privacy dialogue" to analyze the privacy of personal information collected by governments. The dialogue could include a study of the State laws that require the collection of personal information and the Federal laws that require States to collect personal information and consider the desirability of:

1. State enactment of laws similar to the Privacy Act.
2. Extension of the Privacy Act protections to Social Security numbers collected by State governments.
3. Re-evaluation of the meaning of "public records" in light of new technology.
4. A requirement that States redact Social Security numbers and other personally identifiable information from documents before they are placed in the public domain.
5. An Executive Memorandum to State attorneys general reiterating obligations imposed by §7 of the Privacy Act with regard to the protections afforded the collection of Social Security numbers and the requisite notice requirements.

*Why not just do a model state law?*

### **MEDICAL RECORDS/HEALTH INFORMATION**

The confidentiality of health information is a matter of widespread national concern, and the protection of this information has been a priority of the Administration. On September 11, 1997, Secretary of Health and Human Services Donna Shalala recommended that Congress enact Federal legislation to protect the confidentiality of health information by imposing duties on those who hold such information and by providing rights to the subjects of the information. She proposed that the Federal law provide a floor of protection, and that States be permitted to, in addition, provide stronger protections.

Under the recommended legislation, health care providers, those who pay for health care, and those who get information from those entities would have to permit patients to see their own records, to keep records of disclosures and let patients know who has seen their records, and to permit patients to file proposals for correction of erroneous records. All entities collecting or maintaining information would have to advise patients clearly of their confidentiality practices and of the patients' rights.

Disclosures would be limited to those authorized by the patient, or those specifically permitted in the legislation, including disclosures for important public purposes, such as treatment and payment, research, public health, oversight of the health care system, and use in law enforcement or other legal proceedings if permitted by other law. There would be strict limitations on further disclosure in many of these instances. Within an organization, information could be used only for purposes reasonably related to the purposes for which it was gathered, and all disclosures would have to be limited to the minimum necessary to accomplish the purpose of the disclosure.

Entities receiving information pursuant to patient authorization would have to give patients a statement of their intended use of the information, and would be civilly liable for uses in violation of that statement.

There would be civil and criminal sanctions for violations, such as improper disclosure and obtaining information under false pretenses.

Congress is now considering the recommendations.

#### Legislative Proposal

HHS will provide additional proposals for Executive action in the area of medical records/health information.

ok.

what?

### **FINANCIAL INFORMATION**

The recent increase in cross-industry corporate mergers raise important privacy concerns with regard to the treatment of consumer information shared by affiliated companies. Such mergers may allow detailed and sometimes sensitive information about consumers, including medical and financial data, to be shared among newly related companies with relatively few restrictions. In the case of the recent merger of Citicorp and Travelers, for example, consumers might not anticipate that providing information for insurance underwriting purposes to one entity might later be used by the financial institution that is or becomes an affiliate.

Each of the nations' largest 25 banks has a securities affiliate, and banks of all sizes sell insurance. Affiliate information sharing already includes not only sharing of information for

marketing purposes (e.g., a credit card bank soliciting an affiliate broker-dealer's best customers for a new platinum card) but also for security purposes (e.g., tracking a credit card holder's spending patterns in order to detect immediately any unusual activity that might indicate fraud or theft) and increasingly for risk-management purposes (e.g., a customer's record of payment on a credit card apparently is quite useful in determining whether that customer is a good risk for auto insurance). Such practices can be expected to continue, as the lines between various types of financial services firms continue to blur and the firms continue to merge.

The Fair Credit Reporting Act (FCRA) governs activities of agencies that furnish consumer information to consumer reporting agencies and credit or "consumer" reports to third parties. The FCRA defines a consumer reporting agency as a person or entity that regularly assembles or evaluates consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties to be used as a factor in establishing the consumer's eligibility for credit, insurance, employment purposes, etc.

Companies that share consumer information with their affiliates are not subject generally to the controls of the FCRA. This exemption was created in the 1996 Amendments to the FCRA. The FTC raised concerns about exempting consumer information shared by affiliates from the protections of the FCRA. The banking industry was strongly opposed to extending the FCRA protections to consumer information shared by affiliates. In the end, affiliate sharing was permitted, but customers were granted an explicit right to opt out of affiliate information sharing of personal information other than "experience" or "transactional" information (which may be shared not only with affiliates but also third parties). For example, a customer can prevent personal information contained in an account application from being shared.

The 1996 Amendments to the FCRA also contains an odd provision prohibiting the banking agencies from examining for compliance with the Act; rather, they must await a complaint or other indication of trouble. The banking regulatory agencies also are prevented from issuing regulations under the Act, but the Federal Reserve may promulgate "interpretative" opinions in consultation with the other agencies. These provisions were included in 1996 because of banking industry concerns about regulatory burden, as part of the compromise that moved the bill forward. Banks see the prohibition on compliance examinations as putting them on the same footing as everyone else covered by the FCRA.

The OCC, which regulates national banks, has announced its intention to review the disclosure practices of national banks under the FCRA to ensure that the opt-out option is made evident to consumers. The Federal Reserve expects to issue an interpretation of the 1996 Amendments some time this summer that would clarify for all banks what information may be shared with affiliates and how specific and prominent each opt-out notice must be. Treasury has met with the Fed, FDIC and OTS to encourage joint action in this area, and they appeared receptive.

## Proposals

a. The Administration could publicly prod action by national banks to make the opt-out options and notices evident to consumers.

b. The Administration could seek legislation repealing the exemption in the FCRA for affiliate data sharing by financial services firms, or scaling it back -- e.g., permitting information sharing for marketing purposes but not other purposes. (Sharing of the most sensitive type of information -- medical information -- is already addressed above.) For example, businesses could share consumer information among affiliates in connection with a credit card marketing campaign, but consumer information provided for insurance underwriting purposes to one entity could not be used by another entity to deny a person a loan without implicating the protections of the FCRA. This proposal may appease the banking industry, which uses the information mainly for marketing purposes, while still protecting the consumers. The FTC probably would support such action.

*Note: Action in this area must be taken cautiously. The 1996 Amendments were the product of an intense, multi-year debate. Revisiting the affiliate sharing issue would most likely be strongly opposed by the banking industry and may be a sensitive issue on the Hill.*

c. Authorize the appropriate agency to write enforceable rules in this area. Alternatively, give this authority to each of the appropriate agencies to be exercised jointly.

*get nothing out of this.*

## Study Proposals

a. As more databases are available directly to companies, and companies themselves share information directly, there is some concern that the FCRA may become outdated and obsolete. Companies, for example, will no longer purchase credit reports from a central bureau, but rather will obtain information directly from the individual sources and create their own internal credit reports. In the absence of traditional credit reporting agencies, the protections of the FCRA would evaporate. The Administration could undertake a study to determine whether the FCRA contains the protections needed in the electronic age.

b. The Administration could review whether the regulatory review process for mergers should include a consumer protection analysis. For example, in addition to Justice Department review of a proposed commercial merger, the regulating agency could review the proposed merger to determine whether the merger negatively affects consumers' privacy.

## PROFILING

Commercial "profilers" build dossiers about individuals by aggregating information from a variety of database sources, including public and non-public records. Individual reference services, sometimes called look-up services, represent a sub-set of the profiling industry. These services provide information that assists users in identifying individuals, locating individuals, and verifying identities.

Although profiling plainly has legitimate purposes, the public also has legitimate concerns about the compilation of -- and access to -- dossiers that may contain a great deal of personal information about a given individual.

### Best Practices Model – Individual Reference Services Group

On December 17, 1997, a group of 14 Individual Reference Services (the Individual Reference Services Group, IRSG) entered into an agreement on privacy practices which was submitted to the Federal Trade Commission. The IRSG program is based on compliance with certain principles, including notice, disclosure, choice, security, and public education. IRSG members agreed to acquire personal information only from reputable sources, to exclude marketing information as a source, to take reasonable steps to assure that data collected is accurate, complete and timely for the purpose for which it will be used, to correct non-public records when appropriate, and to limit distribution of non-public information to subscribers with appropriate intended uses.

The IRSG committed to implement a rigorous enforcement compliance method. The enforcement program has two prongs. First, signatories' practices are subject to review by a "reasonably qualified independent professional service." On the basis of established criteria, that entity determines whether a signatory is in compliance with IRSG principles. The results of the annual review are made public. Second, signatories who are information suppliers may not sell information to look-up services that do not comply with the IRSG principles.

The IRSG members agreed to provide individuals with access to information contained in services and products that specifically identify them, unless the information comes from a public record, in which case the companies will provide the individuals with guidance on how they can obtain the information from the original source. The FTC strongly disagreed with the limitation on the access provisions of the IRSG practices, and the Commission and IRSG agreed to allow 18 months before revisiting the access issue. On the basis of the IRSG program and the commitment to review access issues, the FTC advised the Congress that legislation on individual reference services was premature.

## Proposal

The IRSG agreement is a good start, but it only covers one category of business involving the compilation of personal information -- traditional "look up" services like those offered by Lexis-Nexis. Other types of entities purchase information from one or more sources to create profiles. For example, some companies are in the business of compiling profiles and reselling them to industry users. Private investigation firms sell identifying and background information collected from public records, interviews, and other investigatory sources. Public records resellers sell public record information like driving and criminal records. List brokers like Metromail gather information in the aggregate from marketing transactions and rent the information typically used for marketing purposes.

The Administration should announce an effort, in conjunction with the FTC, to encourage these other types of entities to adopt self-regulatory principles analogous to those adopted by the IRSG and tailored to their line of business. (Private sector entities that create profiles based on information they collect themselves would be covered by the online privacy self-regulatory initiative discussed above.) The Administration could point out that addressing this issue is important to give individuals the security they need to do business in both the off-line and the on-line environment and that, as with online privacy generally, if the private sector fails to address the issue, the Administration will have to consider whether more direct government intervention is appropriate.

Q upi now?

## **IDENTITY THEFT**

The term "identity theft" generally refers to the fraudulent use of another person's identity to facilitate the commission of a crime, such as credit card fraud. The criminal gathers information about a person and then uses the information to adopt the identity of a victim. The Secret Services reports that this type of offense is growing rapidly, and the victims have been the focus of intense media and Congressional interest.

Under existing law, identity theft offenses are clearly punishable to the extent that they include identification documents (i.e., forged or stolen documents) and an intent to defraud the United States. In other cases, however, there may be gaps in federal or state law that would permit or provide only minimal punishment for the practice.

Thus, it would be helpful to change the law to recognize the potential harm that could be done by offenders who commit identity theft with means of identification, and to address other problems that have emerged as a result of a dramatic increase in cases of identity theft. At the same time, legislation to criminalize identity theft must be carefully crafted to avoid problems that could arise from the federalization of a large new class of crimes.

Last week, Senator Kyl marked up his bill, S. 512, the Identity Theft and Assumption Deterrence Act of 1997. After raising initial concerns about the breadth of the bill, the Departments of Treasury and Justice worked with Kyl to produce a more narrowly focused bill.

#### Legislative Proposal

a. Assuming that the Kyl bill meets remaining Administration concerns, the Administration could endorse the Kyl bill, and work publicly with Senator Kyl and the banking industry (which strongly supports the bill) to see it enacted.

b. Merchants require check-writers to provide proper identification, which often includes a driver's license or other identification card with a social security number. Usually a merchant will record the identifying number onto the check to provide proof of the verification activity. This simple action can create a ream of problems. As a result of this activity, a person's check, which contains a person's name, address, and bank account number, now also contains the individual's social security number. By linking these pieces of personal information together on a single check a merchant has made this customer an even better target for identity theft.

The Administration could seek legislation that makes it illegal to record social security numbers on a check that is being approved for a purchase. This would mirror a law that was passed several years ago that prohibited the recording of a credit card number onto a check when the credit card was used as a piece of identification. Such legislation would neither make it illegal for a merchant to ask for the identification, nor indicate that such a check occurred. The law would merely prohibit writing the actual social security number on the check. Note, however, that modern "telecheck" technology permits merchants to ensure that a personal check is good without a Social Security number.

OK

#### **THEFT OF PERSONAL INFORMATION**

Recent media reports and Chairman Leach have highlighted a problem related to identity theft, where an offender obtains information illegally but then uses it for a *legal* purpose -- e.g., pretends to be a customer in order to trick confidential information out of a bank, and then sells that information to a private investigator, perhaps in a divorce case involving the customer.

#### Option

Chairman Leach will be floating a bill this week to address this problem, and will hold hearings on July 28 in the Banking Committee. At this point, we do not know what the bill will contain, though his staff has promised to provide Treasury a copy as soon as it clears Legislative Counsel. If the bill is acceptable, the Administration could support the bill, and package the support with the Kyl "identity theft" bill.

OK



## PROTECTION OF NEW TYPES OF PERSONAL INFORMATION

The use of Social Security number by the private sector in connection with a variety of transactions allows profilers, marketers and others to combine discrete bits of information to create a portrait of an individual. These portraits have legitimate uses -- law enforcement, credit assessments, debt collection, etc. -- and we therefore must tread cautiously to avoid upsetting an information structure that is fairly well established. The FTC recently indicated to Congress that the use of a unique identifier like Social Security numbers may contribute significantly to the accuracy of these portraits. In addition, the FTC indicated that "the cat may be out of the bag" with respect to private sector use of social security numbers.

Section 7 of the Privacy Act makes it unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number. The Act provides an exception that permits Federal, State or local governments to request disclosure of an individual's social security number. In such cases, the Act requires notice of whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

It seems unlikely that anything can be done with respect to limiting the use of social security numbers by the private sector -- they have become ubiquitous and any limitation could have significant economic implication. On the other hand, as technology provides new means of identification, such as biometrics, it is important to consider how to give individuals more control over these new categories of identifying information.

### Proposal

The Administration could undertake a study (with or without public announcement) to determine whether any steps are necessary to allow individuals to exercise more control over the information that is relevant to new identification technologies.

## PUBLIC EDUCATION

The U.S. approach to privacy focuses on choice -- individuals should have the choice to protect or disclose most personal information. Many Americans are unaware of how their personal information is used, and they do not understand how to protect themselves or exercise their ability to choose. Likewise, many businesses are unaware of consumer concerns about privacy and have not thought through their information handling practices in light of this concern.

## Proposal

The Administration could identify private sector partners to develop an advertising campaign to inform individuals about how to exercise choice with respect to the collection and dissemination of their personally identifiable information. Such a campaign could include all advertising mediums – radio, television, print, and electronic.

- **profiling**

Profilers compile information about individuals and then sell that information. Last December, fourteen such services agreed to abide by principles governing disclosure of nonpublic information. [Note that FTC agreed not to seek legislation in order to allow time to assess this self-regulatory venture.]

- propose legislation requiring that all persons engaged in profiling participate in a self-regulatory system with standards along the lines of the FTC's look-up services agreement.
- give FTC authority to tighten look-up service standards based upon a determination that the existing standards do not strike an appropriate balance between protection of personal privacy and other interests
- propose specific regulatory regime tougher than current agreement

- **marketing**

Marketers purchase various lists to identify targets for mail order/telephone/internet sales pitches. The Direct Marketing Association has adopted a number of principles governing the activities of its members, including a right to opt-out of such solicitations.

- propose legislation requiring that all persons engaged in marketing participate in a self-regulatory system with standards along the lines of the DMA principles
- give FTC authority to tighten standards based upon a determination that the existing standards do not strike an appropriate balance between protection of personal privacy and other interests
- propose specific regulatory regime tougher than current DMA principles

- **children**

- propose legislation prohibiting collection of personal information from children under 13 without prior parental consent

- **credit reporting**

The Fair Credit Reporting Act governs activities of credit reporting agencies that furnish reports to third parties. Act was amended in 1996. As more databases are available directly to companies, and companies themselves share information directly, there is some concern that the Act may become outdated because companies no longer will

# DRAFT

purchase credit reports from a central bureau, but rather will obtain information directly from the individual sources. Also, FTC is concerned that provision of the Act permitting sharing of information between “affiliates” may lead to abuses.

- Announce study to determine whether FCRA contains the protections needed in the electronic age. This study could be broadened to cover all federal laws/regulations governing private sector treatment of personal information.
- **state government data releases**

Federal law prohibits the disclosure of personal information by the Federal government. States are one of the main sources of personal information entering the public domain, because most States do not have privacy laws. Many State FOI/public record laws were created prior to the ease of access to information in the technology era and, in addition, many States sell personal information. Federal laws in some circumstances require States to collect social security numbers and other personal information.

- announce plans to initiate a “privacy dialogue” with the States regarding the privacy of personal information collected by governments.
- analyze the State laws that require the collection of social security numbers and personal information and Federal laws that require States to collect social security numbers and personal information.
- discussions leading up to a privacy summit at which one or more of the following could be discussed and/or agreed to

Suggest that States develop privacy laws similar to the Privacy Act to protect personal information gathered by States

Extend the Privacy Act to social security numbers collected by States.

Ask States to reevaluate and redefine the meaning of “public records” in light of new technology.

Propose that States develop a policy of redacting social security numbers from documents before they are put into the public domain.

Issue a memorandum to public schools reiterating obligations imposed by the Family Educational Rights and Privacy Act of 1974 (“FERPA”). (Under FERPA, public schools that accept federal funds are prohibited from disclosing a student’s social security number and personal information without the student’s consent.)

# DRAFT

- **social security numbers**

The use of the social security number by the private sector in connection with a variety of transactions allows profilers, marketers and others to combine discrete bits of information to create a portrait of an individual. These portraits have legitimate uses -- law enforcement, credit assessments, debt collection, etc. -- and we therefore must tread cautiously to avoid upsetting an information structure that is fairly well established. Also, the FTC recently has indicated to Congress that “the cat may be out of the bag” with respect to private sector use of social security numbers.

- Announce study of private sector use of social security numbers [state governmental use will be addressed through prior initiative]. Study would assess when and why the numbers are requested, whether the purpose is legitimate, whether privacy is considered, if the information is being sold without the individual’s consent, the effect of prohibiting collection of social security number, and whether there is an alternative to the collection of social security numbers. It also would assess the availability and possible use of alternative identifiers, such as biometric information.

- **public service ad campaign**

Our privacy policy relies in large part on choice -- an individual has the option to protect his or her privacy. We should look for private sector partners to develop an advertising campaign to inform individuals of this choice and how to effectuate it. Part of the campaign would be the creation of an electronic one-stop opt out service.

- **identity theft**

[DOJ]

05/28/98 TUE 16:35 FAX 202 326 2558  
05/19/98 FRI 15:44 FAX 202 326 3585

FTC SAT 4  
FEDERAL TRADE

0002  
0002  
PAGE 2

*Eric J. [unclear]*



# SOCIAL SECURITY ADMINISTRATION

Office of the Deputy Commissioner  
for Legislation and Congressional Affairs

May 13, 1998

The Honorable Jerry Kloczka  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Mr. Kloczka:

This letter responds to your request for Social Security Administration (SSA) comments on your bill, H.R. 1813, the Personal Information Privacy Act of 1997. The central focus of the bill appears intended to prevent commercial uses of the Social Security number (SSN) without the number holder's consent.

Although the bill would address valid concerns about the use of the SSN for non-Social Security purposes, the effect of the bill could cause two major problems. The bill would restrict data exchanges which benefit the public; that is, desirable uses of SSNs may extend beyond those exempted from the requirements of the bill. SSA uses these data exchanges to ensure accurate payment of benefits and to reduce fraud. Limitations or foreclosure of such data exchanges could work at cross purposes to SSA program integrity initiatives.

Secondly, the bill is very restrictive considering the extent to which the SSN is already being used in the private sector. Any expense caused by necessary disruptions would likely be borne by consumers.

500 E Street, SW - Suite 800 - Washington, DC 20254-1701  
(202) 358-6024 - Fax: (202) 358-6074

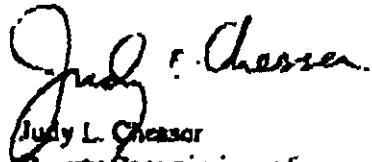
05/26/98 TUE 16:35 FAX 202 326 2558  
05/15/98 FRI 15:44 FAX 202 326 3585

FTC SAT 4  
FEDERAL TRADE

003  
003

The bill's intended limitations on commercial uses of SSN's will contribute to public privacy interests; however, the bill could limit useful governmental exchanges of information for the public benefit and would disrupt the normal flow of business exchanges. My staff would be happy to meet with your staff to discuss our comments.

Sincerely,



Judy L. Chesser  
Deputy Commissioner for  
Legislation and Congressional Affairs

24

003



UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

May 20, 1998

The Honorable Jerry Kleczka  
United States House of Representatives  
2301 Rayburn Building  
Washington, D.C. 20515

Dear Representative Kleczka:

Your letter of April 3, 1998 requested the Federal Trade Commission's comments and possible endorsement of the bill you introduced last year: H.R. 1813, titled the "Personal Information Privacy Act of 1997." The Commission has experience with consumer privacy issues and appreciates the opportunity to review and comment on the proposed legislation. We share your concerns about protecting consumers' privacy, reducing the risk of identity theft, and restricting access to Social Security numbers, and support certain portions of the proposed bill. In light of the Commission's experience and findings in this area, however, the Commission has determined that certain parts of the bill are problematic and prevent our full endorsement of the proposed legislation at this time.

*FTC Activities Related to Identity Theft*

Identity theft, the focus of your legislation, occurs when an individual misappropriates another's name, address, Social Security number, or other identifying information to commit fraud. Even though federal credit card liability protections prevent substantial immediate financial injury, individual victims endure harm that can be severe and long-lasting. Until victims can cleanse their credit reports of the perpetrator's bad acts (a time-consuming and often-difficult process), they may lose the ability to borrow money for houses and cars, and may lose job opportunities.

The Commission is aware of the problems posed by identity theft and has responded in three ways. First, the Commission hosted two public workshops on identity theft to facilitate dialogue among representatives of credit bureaus, credit grantors, law enforcement agencies, consumer and privacy advocates, and consumer victims concerning this crime.<sup>1</sup> Second, as

---

<sup>1</sup> The transcript of the Commission's first Meeting on Consumer Identity Fraud, held in Washington, D.C., August 20, 1996, is available on the Commission's Web site at *Federal Trade Commission, Conferences* (last modified Mar. 14, 1998) <<http://www.ftc.gov/ftc/conferences.htm>>. There is no transcript of the second meeting, held in November 1996. Attendees split into working groups with FTC staff as facilitators for each group. The



The Honorable Jerry Kleczka -- Page 2

discussed in more detail below, the Commission conducted a study of issues arising from computerized database services that make available personal identifying information about consumers, also known as "individual reference services" or "look-up services." Commission staff has also worked with members of that industry to encourage them to develop and adopt meaningful self-regulation. Finally, the Commission is engaged in ongoing efforts to educate consumers and business about these important issues.<sup>2</sup>

The Commission began to focus on identity theft in the fall of 1996, as computerized database services were drawing considerable public and media attention. At issue was the sensitivity of the information these services gather about consumers and the ease with which this information could be accessed. In connection with pending amendments to the Fair Credit Reporting Act ("FCRA"), Senator Bryan solicited the Commission's views on the sale by credit bureaus of the personal identifying information found in look-up services. As your letter notes, the Commission responded on September 23, 1996, recommending additional amendments to the FCRA that would limit release of certain identifying information, including Social Security numbers, only to those credit bureau subscribers who would otherwise have a "permissible purpose" under the FCRA to receive a full credit report.

Rather than incorporate this suggestion into the pending legislation, Congress directed the Federal Reserve Board to study the impact of the misuse of this sensitive information on insured depository institutions.<sup>3</sup> In addition, Senators Pressler, Bryan, and Hollings requested that the Commission conduct a study of these computerized database services.<sup>4</sup> Because the study would examine the potential risks posed by the sale of personal identifying information by credit bureaus, the Commission withdrew its earlier legislative recommendation to Senator Bryan until there had been an opportunity to analyze the results of the study.

In March 1997, the Commission announced its plan to conduct a study of look-up services.<sup>5</sup> The Commission gathered information regarding the look-up services industry

---

groups discussed prevention, detection, and correction issues as well as consumer and business education.

<sup>2</sup> See, e.g., *Federal Trade Commission, Identity Thieves Can Ruin Your Good Name*, (last modified May 11, 1998) <[www.ftc.gov/bcp/online/pubs/credit/identity](http://www.ftc.gov/bcp/online/pubs/credit/identity)>.

<sup>3</sup> Federal Reserve Board Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud (March 1997).

<sup>4</sup> Letter from Senators Larry Pressler, Richard H. Bryan, and Ernest F. Hollings to Commission (October 8, 1996). They requested that the study encompass the collection, compilation, sale, and use of computerized databases that contain consumers' identifying information, without their knowledge. *Id.*

<sup>5</sup> 62 Fed. Reg. 10,271 (March 6, 1997).

The Honorable Jerry Kleczka -- Page 3

primarily by soliciting public comment and holding a workshop in June 1997. The Commission learned that look-up services, if not adequately controlled, pose certain risks. Consumers may be adversely affected in three ways: (1) by a privacy infringement, including uses of their information inconsistent with the purpose for which they initially provided it; (2) by the reliance of others on inaccurate information contained in the databases; and (3) by the wrongful use of their information to commit fraud, such as identity theft. At the same time, the Commission found that look-up services confer benefits on legitimate users. For example, access to identifying information through look-up services helps banks and creditors prevent fraud, including identity theft; helps private investigators track down witnesses; and helps public interest groups search for missing children and non-custodial parents owing child support. In addition, the Commission learned that news reporters as well as federal, state, and local law enforcement agencies rely on information obtained through commercial look-up services to assist their investigations.

#### *The IRSG Principles*

At the June workshop, industry members announced that they had formed the Individual Reference Services Group, or "IRSG," and presented an initial self-regulatory proposal intended to address public concerns about their databases. Over the next five months, Commission staff worked with members of the group to encourage them to adopt a more effective self-regulatory program. On December 15, 1997, the group signed and released the Individual Reference Services Group ("IRSG") Principles -- a comprehensive set of self-regulatory guidelines agreed to by most of the industry. In a December 1997 report to Congress on look-up services,<sup>6</sup> the Commission recommended that additional legislation not be introduced until the effectiveness of the IRSG Principles has been evaluated.<sup>7</sup>

Although the IRSG Principles will not become effective until December of this year, they represent an important attempt to regulate access to identifying information that is obtained from *non-public* sources and is not otherwise publicly available. 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 and therefore not restricted under the IRSG principles.

---

<sup>6</sup> *Individual Reference Services: a Report to Congress* (December 1997). The report can be found online at *Federal Trade Commission, Privacy, Reports, Guides, Letters, and Policy Statements* (last modified May 11, 1998) <<http://www.ftc.gov/privacy/reports.htm>>.

<sup>7</sup> We note that at the time your bill was proposed, the industry had not yet agreed to self-regulation addressing certain concerns in this area.

The Honorable Jerry Kleczka -- Page 4

Restrictions on access to information vary according to the following three categories of customers:

- The general public may not access, over the Internet or in any other context, sensitive, non-public information (a concern expressed in your letter). This prohibition covers Social Security numbers, date of birth, mother's maiden name, and unlisted telephone numbers, to the extent such information is not otherwise publicly available.
- Entities who are legitimate commercial firms but who do not have a demonstrable need for sensitive information (like full Social Security numbers) may access only truncated Social Security numbers.
- Only firms who have been screened by IRSG signatories and who can demonstrate a legitimate need for the information sought may access non-public, sensitive identifying information, such as Social Security numbers, date of birth, and mother's maiden name obtained from credit bureaus.

The approach incorporated in the IRSG Principles shows particular promise because all three major credit bureaus are signatories. These credit bureaus are the principal source of potentially sensitive, non-public information for the look-up industry. By signing the Principles, they have agreed to refrain from selling such information to firms that fail to comply with the IRSG Principles, regardless of whether those firms are signatories to the Principles. We believe the IRSG Principles, while not perfect, have the potential to accommodate the legitimate uses of look-up services while addressing many concerns about consumer privacy and identity theft.

#### *Discussion of Relevant Sections of Proposed Personal Information Privacy Act of 1997*

The bill has three principal sections: Section 2 would amend the FCRA to treat certain identifying information essentially as part of a consumer or credit report. Section 3 would prohibit the purchase, sale, and commercial use of Social Security numbers without consumers' consent. Finally, Section 4 would restrict use of Social Security numbers by state departments of motor vehicles.

#### *Section 2: Confidential Treatment of Credit Header Information*

Section 2 seeks to extend coverage of the FCRA to Social Security numbers, date of birth, and mother's maiden name contained in credit headers.<sup>5</sup> Access to this identifying

---

<sup>5</sup> A credit header is the portion of a credit report containing identifying information, typically including name, aliases, current and former addresses, phone number, Social Security number, date of birth, and mother's maiden name.

The Honorable Jerry Kleczka -- Page 5

information would be provided only to those entities who qualify as having one of the limited "permissible purposes" defined by the FCRA. However, the FCRA definition does not include law enforcement, fraud prevention, news reporting, the search for missing children, or many other legitimate uses of identifying information and thus would prevent private and public investigators seeking to accomplish these tasks from accessing complete credit header information.<sup>9</sup>

As discussed previously, by the end of this year the signatories to the IRSG Principles will begin self-regulating the commercial sale of non-public personal identifying information collected by them. Last year, the Commission concluded that the IRSG Principles showed promise for effectively regulating the availability of non-public personal identifying information, including credit header information, and recommended that legislation be postponed until the viability of the IRSG self-regulatory scheme has been evaluated.

*Section 3: Prohibiting Purchase, Sale, and Commercial Use of the Social Security Number without Consent*

The Commission has several concerns about prohibiting the purchase, sale, and commercial use of Social Security numbers without the consent of the individual. The Commission learned through its study of look-up services that many non-profit organizations, government, and other non-commercial entities such as news reporters, private investigators, and attorneys purchase Social Security numbers from look-up services in connection with law enforcement and, for example, searches for missing children, witnesses, or parents owing child support. These entities informed the Commission that they require the most inclusive information possible. If individuals could choose not to be included in the databases, over time the databases might become limited to identifying information about only the most law-abiding citizens. The Commission also learned that some commercial uses of Social Security numbers have important societal benefits. The financial industry, for example, accesses Social Security numbers to verify the identity of loan applicants and account holders, and thereby to prevent fraud, including identity theft.

In addition, Social Security numbers, as personal and unique identifiers, help entities like hospitals, banks, universities, and credit bureaus link the right persons to their records, and thereby avoid matching data to the wrong persons. In the credit reporting industry, for example, correct attribution of credit information is necessary for accurate credit bureau files. Credit bureaus have files on over 200 million people. Every month, credit grantors supply new and

---

<sup>9</sup> The FCRA does permit government agencies to obtain limited information (name, addresses, and employment), 15 U.S.C. § 1681f, but access to full credit header information would be permitted only by court order if this bill were enacted. In addition, state or local government child support enforcement agencies can obtain a full consumer report for certain purposes. 15 U.S.C. § 1681b.

The Honorable Jerry Kleczka -- Page 6


updated information to those credit bureaus. Often, a Social Security number is the key to matching the new data to the old file, especially for consumers who have moved, changed names, or have names similar to those of their children or parents. Prohibiting the nonconsensual use of Social Security numbers, without some substitute form of identification, could affect the accuracy of credit bureau files, and in turn, consumers' ability to get credit, employment, and insurance.

*Section 4: Restriction on Social Security Number Use by Motor Vehicles Departments*

The Commission, in its study of look-up services, found that easy access to sensitive, unique information (e.g. Social Security number) listed on certain public records increases the risk of serious harm to consumers, including identity theft and stalking. Amending the Driver's Privacy Protection Act to further limit the distribution of Social Security numbers by state departments of motor vehicles, to the extent it does not interfere with beneficial uses of Social Security numbers by government, is a positive step toward addressing that concern. Government agencies may not have 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 public dissemination of that information is not essential to advance their intended purpose in collecting the information in the first place. The Commission has encouraged public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices.

The Commission shares your concerns about the improper use of Social Security numbers, particularly when misappropriated to commit identity theft. Government and industry must acknowledge that the extensive commercial dissemination and use of Social Security numbers pose serious concerns and merit continued attention. Nonetheless, the broad prohibitions set forth in the proposed bill may have unintended, negative consequences. It might be beneficial at this time to monitor and even encourage the development of alternative methods of identification that might pose fewer risks. For example, participants at Commission workshops have reported on-going progress with biometrics and digital signatures.

By direction of the Commission.

  
Robert Pitofsky  
Chairman

Attachment:

February 28, 1997 letter from Chairman Pitofsky to Senator McCain

# Individual Reference Services Group

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 fully, 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.

43 **PRINCIPLES:**

44

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

49

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

52

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

55

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

62

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

66

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

71

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

76

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

79

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

86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128

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 dissemination 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



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

- 133
- 134 1. NON-PUBLIC INFORMATION products or services distributed pursuant to this  
135 subsection shall not include:
- 136
- 137 a. Information that reflects credit history, financial history, medical  
138 records, mother's maiden name identified as such, or similar  
139 information;
- 140
- 141 b. Certain information like social security number and birth information  
142 unless truncated in an APPROPRIATE and industry consistent manner.
- 143
- 144 2. Users shall agree to terms and conditions consistent with these principles prior  
145 to accessing the NON-PUBLIC INFORMATION, shall agree to use such information  
146 solely in the normal course and scope of their business or profession and that the  
147 use is APPROPRIATE for such activities and that they shall limit their use and  
148 redissemination of such information to such uses and in accordance with these  
149 principles.
- 150
- 151 3. Individual reference services shall take reasonable steps to protect against  
152 misuse of the NON-PUBLIC INFORMATION distributed pursuant to this subsection  
153 which will include:
- 154
- 155 a. If not previously established, the individual reference service shall take  
156 reasonable steps to identify the user and to establish the user as an  
157 established professional or commercial entity.
- 158
- 159 b. Reasonable measures shall be employed to help assure that commercial  
160 and professional customers use NON-PUBLIC INFORMATION  
161 APPROPRIATELY.
- 162
- 163 c. Individual reference services shall implement reasonable mechanisms to  
164 remedy subscriber abuses of the information.
- 165
- 166 d. Individual reference services shall maintain a record of the identity of  
167 subscribers and the terms and conditions agreed to by the subscriber for  
168 three years after termination of each subscriber's relationship with the  
169 individual reference service.
- 170

171 C. *General Distribution of Non-Public Information:* Individual reference services, when  
172 they limit the NON-PUBLIC INFORMATION content of their products or services as set  
173 forth in this subparagraph, may distribute such products or services to any person.  
174

175 1. NON-PUBLIC INFORMATION distributed pursuant to this subparagraph shall not  
176 knowingly include information that reflects social security number, mother's  
177 maiden name identified as such, non-published telephone number, or non-  
178 published address information obtained from telephone companies, birth  
179 information, credit history, financial history, medical records, or similar  
180 information, nor will the service be retrievable by a social security number.  
181

182 2. The individual reference service shall take reasonable steps to protect against  
183 the misuse of NON-PUBLIC INFORMATION.  
184

185 VI. *Security:* Individual reference services shall maintain facilities and systems to protect  
186 information from unauthorized access and persons who may exceed their authorization. In  
187 addition to physical and electronic security, individual reference services shall reasonably  
188 implement:  
189

190 A. Employee and contractor supervision—Employees and contractors shall be required to  
191 sign confidentiality agreements and be subject to supervision.  
192

193 B. Reviews—System reviews shall be made at APPROPRIATE intervals to assure that  
194 employees are complying with policies.  
195

196 VII. *Openness:* Each individual reference service shall have an information practices policy  
197 statement that describes what types of information it has, from what types of sources, how it is  
198 collected, the type of entities to whom it may be disclosed and the type of uses to which it is put,  
199 and shall make its policy statement available upon request. Consumers shall be notified about  
200 these practices in various ways such as:  
201

202 1. Web sites;  
203

204 2. Advertisements; or  
205

206 3. Company or industry-initiated educational efforts.  
207

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

214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242

- IX. *Access*: Upon request and reasonable terms, 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 report and any subsequent actions taken or response made by the company shall be publicly available.

243 **PLEDGE:**

244

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

247

248

Axiom Corporation

249

CDB Infotek, a ChoicePoint Company

250

DCS Information Systems

251

Database Technologies, Inc.

252

Equifax Credit Information Services, Inc.

253

Experian

254

First Data Solutions Inc.

255

Information America, Inc.

256

IRSC, Inc.

257

LEXIS-NEXIS

258

Metromail Corporation

259

National Fraud Center

260

Online Professional Electronic Network

261

Trans Union Corporation

ment to act on failure of American companies to ensure  
 er privacy By Frank James Chicago Tribune (KRT)  
 SHINGTON The failure of many American companies to  
 re consumer privacy as they gather personal and often sensitive  
 information about millions of people for marketing purposes is raising  
 pressure for federal government action.

By early summer, as part of an administration assessment of how the  
 internet is progressing as a place to buy and sell, Commerce Secretary  
 William Daley must report to President Clinton on how well firms are  
 policing themselves in handling personal information.

If he had to grade them now, they would likely get a failing grade.  
 "It's not going very well," he said of self-regulation efforts.

The administration perceives a lack of urgency on the part of the  
 private-sector generally, despite numerous administration urgings that  
 corporate officials take concerted action to protect privacy. "Basically,  
 nothing has happened," said a senior administration official who asked  
 not to be identified. "American business is not the most pro-active  
 animal in the world."

The administration had expected the private sector to establish rules  
 to address a range of worrisome privacy concerns. Those include the  
 collection of personal information from children at certain web sites or  
 the frequent inability of consumers to know what information is  
 gathered about them, its accuracy and how it is used.

The private-sector's inertia, the official said, would likely lead the  
 administration to conclude on July 1 when the report to Clinton is due,  
 that "it doesn't look like self-regulation worked. We have to consider  
 other alternatives, (which) would be a shame" he said, referring to the  
 prospect of government regulations.

Corporate America's general failure to boldly show it means  
 business when it comes to protecting the electronically stored personal  
 information about millions of Americans could hardly come at a worse  
 time.

In October, a stringent new privacy law is scheduled to take effect in  
 the European Union. The European Directive on the Protection of  
 Personal Data requires each EU member nation to pass legislation to  
 shield data about individuals. One provision bans personal data from  
 being exported from EU nations to non-member countries where  
 security measures are inadequate.

This might bar U.S. companies from collecting and transmitting data  
 about European consumers, placing them at a distinct disadvantage  
 with their European counterparts.

While European nations view government action as the best  
 safeguard for personal information, the U.S. government prefers  
 self-regulation.

"Nearly 10,000 web sites a week are coming and going. The ability  
 to enforce a law that said 'Thou shalt not collect information from  
 anybody without telling them exactly what you're going to do with it,'  
 would not realistically be enforceable," said Becky Burr, acting  
 associate administrator in the Commerce Department's National  
 Telecommunications and Information Administration.

"If you pass a law that you can't enforce you give people a false  
 sense of security and you eliminate incentives that they have to protect  
 themselves," Burr said.

But with the American approach so far yielding unimpressive  
 results, the Clinton administration will likely have a difficult time  
 persuading the Europeans that personal data is adequately protected in  
 the U.S.

Some privacy advocates viewed Vice President Gore's call at New  
 York University's commencement earlier this month for an  
 "electronic bill of rights" to protect individual privacy as largely  
 aimed at the Europeans.

In his speech, Gore reintroduced already announced administration  
 initiatives, like a soon-to-be-held White House conference on privacy  
 and legislation to protect medical information.

"He was attempting to package it looking towards the Europeans to  
 try and convince the Europeans that there are some substantive  
 improvements happening in the U.S.," said David Banisar, counsel at  
 the Electronic Privacy Information Center in Washington, D.C., an  
 organization that encourages privacy in the computer age. "But the  
 Europeans aren't dumb."

Beyond satisfying the Europeans, U.S. companies are going to have  
 to satisfy Americans too.

In a Business Week/Louis Harris survey of 999 adults in February,  
 61 percent of non-Internet users said they would be more likely to use  
 it if they were assured their personal information would be kept  
 private.

And in an ominous note for American companies, about 53 percent  
 of those surveyed felt lawmakers needed to take immediate action to

control what personal data businesses collect and how it is used.

Some public sentiment is fueled by disclosures of how companies  
 are using personal information in ways most consumers never  
 expected.

For instance, the CVS drug store and Giant supermarket chains  
 recently drew the ire of customers after reports that the companies  
 sold personal medical information gleaned from filling prescriptions to  
 a marketing company, Elensys Inc. of Woburn, Mass. Knowing what  
 customers were prescribed helped Elensys market other drugs for the  
 same condition.

The uproar caused Giant to stop sending such information to Elensys  
 while CVS offered customers the chance to opt out.

While the mining of databases for information to help marketers  
 predates the Internet, the global network has accelerated the concerns.  
 For it can be an effective tool for gathering sensitive personal  
 information from visitors to web sites, including children. And it  
 makes distributing such data almost effortless.

Meanwhile, more powerful computers give marketers the ability to  
 sort data about people in previously unheard of ways, giving them the  
 ability to create detailed profiles of individuals' habits, personal  
 histories and identifying information.

To reassure Americans in the information age Ira Magaziner, the  
 president's adviser on electronic commerce issues, suggests  
 companies with strong privacy policies adopt something like a "Good  
 Housekeeping Seal of Approval." Besides giving consumers  
 confidence, it would give companies with such policies a competitive  
 advantage.

"Seals belong in the zoo," said Harold McGraw III, president and  
 chief executive officer of McGraw-Hill Cos., the large, New  
 York-based information-services company which has taken a  
 leadership role on personal-data privacy issues. He believes seals  
 would prove confusing and lack the credibility they once had.

He favors a simple policy statement that, if violated, could make the  
 company liable for consumer fraud, if nothing else. McGraw-Hill Cos.  
 has created a comprehensive policy.

It requires telling people what information is being gathered and for  
 what purpose. It also calls for "extra care" from McGraw-Hill in  
 handling sensitive personal data like Social Security numbers, a  
 mother's maiden name, personal finances, medical conditions and  
 "most information about children."

McGraw-Hill cannot distribute such information externally. People  
 can even "opt out" of having this information shared among business  
 units within McGraw-Hill. And in the future, the company plans to  
 allow individuals to review and correct, if needed, personal  
 information in its databases.

"When you talk about the whole notion of electronic commerce and  
 the speed at which it's going to transform (business), you've got to be  
 able to get after behavior at the individual level," of companies,  
 McGraw said, noting the difficulty of law-makers and law enforcers  
 keeping pace with the fast-evolving Internet.

"It's going to be very important for industry to make a very strong  
 statement of self-regulation, and live by it," McGraw said.

**Professor defies the odds; experiences 50 percent remission from  
 cancer By John Crewdson Chicago Tribune (KRT)**

LOS ANGELES Barry Riccio might be an anomaly. Then again, he  
 might represent the future of cancer treatment. Either way, Riccio, a  
 professor of American intellectual history at Eastern Illinois  
 University, is not only still alive, he's "feeling much better, thanks."

According to data presented last week at the annual meeting of the  
 American Society of Clinical Oncology here, more than two years  
 after being told his cancer was terminal, Riccio has experienced a 50  
 percent remission. He is the apparent beneficiary of a new approach to  
 cancer treatment which focuses on the blood vessels that feed a  
 malignant tumor rather than the tumor itself.

The idea that cancer could be treated by halting angiogenesis, as the  
 formation of blood vessels is known, was first proposed in 1971 by  
 Dr. M. Judah Folkman of Harvard University and Children's Hospital  
 in Boston. The idea's principal appeal is that, rather than viewing  
 cancer as hundreds of distinct diseases that require individualized  
 treatments, it might be possible to attack all cancerous tumors by  
 targeting the thing they require in common: access to the body's  
 life-giving blood supply.

Over the last decade Folkman has discovered several substances,  
 including the natural proteins he calls angiostatin and endostatin,  
 which make tumors in mice shrink or even disappear by choking off  
 their blood supply.

Although angiostatin and endostatin have not yet been tested in

humans, other researchers following in Folkman's footsteps are pursuing different approaches to the same goal with the tools of genetic engineering, and a few are already testing their discoveries in a handful of cancer patients like Riccio.

Riccio learned he had cancer in September 1993, when he "woke up and looked in the mirror and saw that I was yellow. It was a very hot and humid day, and I just assumed I was reacting to the weather. Later on that evening I attended a party. That's where I fainted."

Riccio's doctors told him he had a tumor in his stomach, "a very rare and unpredictable form of cancer" known as leiomyosarcoma. Surgeons took the tumor out, only to discover a year later that the cancer had spread to Riccio's liver.

"At that point the doctors in central Illinois were not quite certain what to do," recalled Riccio, who was then living in Urbana with his wife, Kathryn Anthony, a professor of architecture at the University of Illinois. "Because there was very little experience with my kind of cancer over there, they weren't sure where I should go."

Some library research led Riccio to the M.D. Anderson Cancer Center in Houston, where in late 1994 surgeons removed a portion of his cancerous liver, leaving the rest intact for fear of damaging crucial blood vessels. Chemotherapy treatments followed, and Riccio says the therapy "wasn't especially kind or gentle. I was in a fair amount of pain, but it was manageable. I thought it was worth it because the tumors were shrinking."

As often happens, Riccio's tumors eventually developed resistance to the cancer drugs, and Riccio's Houston surgeon told him "to come back when my cancer began growing again." A month later, Riccio's wife stepped into the bathroom to find her husband unconscious in the shower, "pale and ashen, my lips purple and my eyes quivering."

Surgeons removed a new tumor that had erupted in Riccio's stomach, taking a third of his stomach along with it. But the cancer in Riccio's liver remained, and soon it had spread to his belly cavity.

Because of the sensitivity of the liver and other abdominal organs to radiation, radiotherapy treatments weren't possible, and Riccio's doctors in Houston pronounced what sounded like a death sentence. "They told me there was nothing more they could do but monitor my situation and prescribe pain medication when the time came," he said.

Three physicians at the Mayo Clinic in Minnesota could offer no better solutions. Loath to simply wait for death, Riccio found a surgeon in Detroit who agreed to remove his belly cavity cancer, but who concluded that the liver cancer was inoperable. "He said, 'I've run out of options,' Riccio recalled. "So this was the third time I was being given bad news."

By coincidence Riccio's father-in-law, who lives in La Jolla, Calif., about 50 miles south of here, had seen a newspaper article about an anti-angiogenesis drug called LM-609 that was being studied at the Scripps Research Institute there.

Developed by Scripps researcher David Cheresh, LM-609 is a bioengineered antibody that inhibits the formation of tumor-associated blood vessels in mice by interfering with the cells that line the vessels. When Barry Riccio contacted Cheresh in late 1996 he learned that LM-609 was about to be tested on humans for the first time.

In January 1997 Riccio, his cancer now having spread to his spleen, drove to California. A few days after arriving in La Jolla Riccio became the second person in the world to be treated with LM-609, known commercially as Vitaxin.

The Vitaxin trial was short one 90-minute infusion a week for six weeks and intended only to see whether patients with advanced cancer of the breast, colon, lung, kidney and cervix suffered any toxic reactions from the compound. According to the data presented in Los Angeles, the side effects of Vitaxin were limited to a brief, mild fever. Although one patient died four weeks after completing the trial, the study's organizers described the death as "unrelated to Vitaxin therapy."

Cheresh and the other researchers hadn't expected to see improvement in any of the patients during such a brief study, and in five of 12 patients the cancer continued to grow. To Cheresh's surprise, however, in six others tumor growth stabilized. In Riccio, they actually began to shrink.

There wasn't enough Vitaxin to keep treating all the patients whose cancers appeared to respond to the drug. But there was enough to treat one, and Cheresh asked the Food and Drug Administration for permission to continue Riccio on Vitaxin therapy on a "compassionate" basis.

During the three months it took the FDA to say yes, Riccio's liver tumors once again began to enlarge an indication, Cheresh believes, that Vitaxin was responsible for his improvement.

When Riccio resumed Vitaxin in June 1997 his tumor shrinkage also resumed, and he is still taking the drug. His oncologist, Dr. John

Gutheil of the Sidney Kimmel Cancer Center, estimates that approximately half as much tumor in Riccio's body today as he began treatment with Vitaxin.

"I am much better now than I was a year ago, or 9 months ago, or even 6 months ago," says Riccio, who is living in La Jolla with his wife and walking three miles a day while he waits to see whether a three-fold increase in his Vitaxin dosage can shrink his tumors even more.

"He came out here with the understanding of just renting an apartment," Cheresh says. "He was, of course, terminal. He'd had five surgeries and all kinds of other therapies, everything a human can possibly tolerate in terms of cancer therapy."

"This was his last hope," Cheresh said. "He's been here now a year and three months. He's doing very well, and you can't convince him that Vitaxin hasn't made the difference."

Whether it has, of course, remains to be seen. Riccio's dramatic improvement might be due to Vitaxin, or to some unrelated phenomenon. As with any experimental drug, the answer lies in a larger, longer clinical trial that compares Vitaxin with established cancer therapies in many patients over many months.

Such a trial is expected to begin early in 1999, but Cheresh says it should take another year to reach any firm conclusions.

Anti-angiogenic therapy, he says, is "like turning the sprinkling system off your front lawn. The grass doesn't die right away."

---

### Community in shock over church explosion By Graeme Zielinski and Abdon Pallasch Chicago Tribune (KRT)

OAKWOOD, Ill. Seven miles away from the calm of a red-brick church here was a place of calamity, where in Danville, Ill., shell-shocked members of the First Assembly of God congregation were convulsed in the horror of a near-deadly bombing during their Sunday services.

But the almost languid scene at the Oakwood United Methodist Church turned to shock shortly after Pastor Bill Adams finished delivering the benediction to the small congregation. That's when a phone call came with news, whispered into his ear, which Adams repeated from the podium.

"He asked for everyone's attention to let us know that there had been an explosion at a Danville church, probably a bomb," Wanda Plawer said. "If we didn't have carpet in our sanctuary, I think you could have heard a pin drop."

That is not only because of the natural shock at what federal authorities confirmed Monday was an act of terrorism that sent 33 Danville worshippers to the hospital, two of them with serious injuries.

"We were very grateful that no one in Danville was killed," Plawer said.

That was not the case when a similar blast hit the Methodist congregation here. On a cold December afternoon less than five months earlier, Plawer's husband, Brian, was killed by a bomb set outside the church's doors.

After the news sunk in, Adams led an emotional prayer.

Though authorities said Monday it did not appear the two bombings were related, throughout the blue-collar community, anchored by Danville, a city of 34,000, less than 120 miles south of Chicago, the oddity and terror of these unsolved crimes was a coincidence that seemed to be on everyone's lips. It also was a source of fear and frustration.

"You can't go to school and you can't go to church. You don't dare go to a post office," said Rick Koss at a Memorial Day prayer service at a cemetery in Danville. "What's the world coming to?"

Beyond confirming it was a powerful man-made device that gashed a hole in the First Assembly of God church Sunday, hurling debris more than the length of a football field away, officials were mute Monday on who may have set the bomb and why.

"We have no suspects in custody at this time," said Larry Thomason, spokesman for the Danville Police Department. Asked if there were any suspects at all, he replied, "There have been interviews, but I can't say whether any (of those interviewed) were suspects."

At a news conference earlier in the day, the church's pastor, Dennis Rogers, said he did not believe there was a link between the bombing and crack houses the church had displaced years earlier as it expanded.

And authorities appeared to discourage speculation linking the Danville bombing to the placement of the deadly Oakwood device set Dec. 30.

"Church bombings in this country are extremely rare," acknowledged Jerry Singer, spokesman for the federal Bureau of