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 whre 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).

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.

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 created 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 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.

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.

SOCIAL SECURITY NUMBERS

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.

Option

The Administration could announce a study that both looks backward -- to discern "lesson learned" from the social security experience -- and looks forward, to avoid the same result with respect to new identification technologies.

COMMERCIAL MARKETING

Please note that we do not propose action at this time in the area of commercial marketing.

Commercial marketers are individuals or entities that:

E. Promote, sell, or deliver goods or services through direct sales marketing, campaigns to increase brand awareness, and other similar marketing strategies;

F. Perform market research; or

G. Foster the promotion, sale, or delivery of goods and services through the sale, rental, compilation, or exchange of lists.

Best Practices (principles) – Online Privacy Alliance, Direct Marketing Association

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.

Best Practices (enforcement) FTC Enforcement, BBBonline, TRUSTe

The marketing industry has made progress by adopting robust statements of fair information practices, but effective self-regulatory enforcement mechanisms are just beginning to emerge.

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 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.

Legislative Option

The Administration could call for legislation that would specify a set of fair information practices applicable to commercial marketers 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 – marketers 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.