MEMORANDUM

TO: Tom Kalil

FROM: Andrew Pincus (Becky Burr, Paula Bruening, Dawn Friedkin)

DATE: July 2, 1998

RE: Privacy – Legislative and Other Options

This memorandum outlines a series of options for legislative and public education proposals for enhancing privacy protection. The Department of Treasury has separately forwarded a memo on the financial services sector.

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.

COMMERCIAL MARKETING

Commercial marketers are individuals or entities that:

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

B. Perform market research; or

C. 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.

INFORMATION ABOUT CHILDREN

The solicitation of information from children presents a unique problem. Unlike adults, children 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 childrens' privacy online.

Best Practices Model – Online Privacy Alliance

On June 22, 1998 the Online Privacy Alliance issued specific guidelines for the protection of childrens' 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 childrens' 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 be presumed to be in compliance with the Federal Trade Commission Act.

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 corporate 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 financial services industry opposition to this issue, this may be difficult. 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 to make 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 would probably also

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.

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 nonconsensual 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, most States do not have analogous privacy laws. Not only is the protection of information collected and maintained by State governments provided 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.

Options

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. The Administration could announce plans to initiate a "privacy dialogue" with the States about 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 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.

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. 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. The Commission has also indicated that use of a unique identifier like Social Security numbers may contribute significantly to the accuracy of those profiles.

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 the Federal, State or local governments to request disclosure of an individual's social security number, but only if required by law. 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.

Unlike section 3 of the Privacy Act, which protects personal information, for which OMB has oversight authority, there is no oversight authority for section 7. When an individual, therefore, has a question with his or her rights with regard to disclosure of his or her social security account number there is no place to go for guidance and/or enforcement.

Additionally, unlike section 3, section 7 addresses only the collection of social security numbers, not disclosure. There is no law that prohibits disclosure of social security numbers.

Legislative Options

a. The Administration could seek legislation to expand the Privacy Act to give social security numbers the same protections afforded the information provided by the Privacy Act.

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 bank account number, no also contains the individual's social security number. By linking these pieces of personal information together a merchant has made this customer a potential target for identity theft, bank fraud, or various other related crimes.

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.

Study Option

The Administration could announce study of private sector use of social security numbers. (State governmental use will be addressed through state data release initiative). The 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 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.

To: Tom Kalil
From: Rick Carnell, Greg Baer
Re: Privacy issues in the financial system

Set forth below, for use at the next Working Group meeting, is a discussion of some privacy issues raised by practices in the financial services industry. The document is probably more detailed than would be needed for a Deputies meeting, but we thought some background in this area would be useful for the Working Group.

Sharing of Confidential Information with Third Parties -- e.g. Direct Marketers

- Although consumers may have some concern in this area, financial services firms represent to us 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.
  - First, the most likely purchasers of such information are the firm's competitors.
  - Second, financial firms fear that their customers would react badly if they learned that their information was being sold.
  - Third, sale of such information is generally prohibited by State common law, as the financial institution, acting as the agent of the customer, owes that customer a fiduciary duty and is prohibited from misusing information obtained from the customer in connection with the agency. The NASD-R also recently proposed a new confidentiality rule for securities firms.
- (When it comes to direct marketing by the financial institution itself, the Fair Credit Reporting Act (FCRA) requires that customers be allowed to opt out of receiving pre-approved offers of credit cards or other credit, and NASD and FTC rules restrict the ability of securities brokers to cold call customers by, among other things, requiring the maintenance of "do-not-call" lists.)

  Recommendation: Take no action unless this area becomes a problem.

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

Sharing of Information with Affiliated Companies

- Currently, each of the nations' largest 25 banks has a securities affiliate, and banks of all sizes sell insurance. Inter-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 Fair Credit Reporting Act, customers have an explicit right to opt out of inter-affiliate information sharing of personal information other than "experience" or "transactional" information (which may be shared not only with affiliates but also third parties). This limited right was brokered as part of the 1996 amendments to the Fair Credit Reporting Act.

  - Thus, 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.

- The FCRA also contains a rather 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.

Recommendation:

- 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.

- 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.

Caveat: 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.

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.

Recommendation: Endorse the Kyl bill and work with him toward passage, provided that the reported version adequately address concerns of the Treasury and Justice Departments.

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: Explore whether the FTC has 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.

On-Line Disclosures

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

- The Office of the Comptroller of the Currency (OCC), a Treasury bureau that regulates the nation's national banks, has announced that it will consider promulgating voluntary guidelines for national banks to use in constructing their web sites, and the FDIC's E-banking Task Force is surveying web sites of FDIC-insured institutions to verify, based on a much larger survey group, whether the results of the Federal Trade Commission's recent survey accurately reflects the practices of the nation's smaller state banks that the FDIC regulates (and it apparently does).

- Main Treasury has met with each of the federal banking agencies (OCC, FDIC, Fed, and OTS) to discuss the scope for 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.

- At our meeting, the banking agencies agreed to coordinate informally their previously independent efforts at establishing guidelines and examiner guidance with respect to banking industry privacy disclosures, in particular on-line disclosures.

Recommendations:

- Such consultative efforts could be officially encouraged, and more formal coordination efforts could be officially recommended.

cc: Commerce Department
Sarah Rosen

THE WHITE HOUSE

WASHINGTON

June 24, 1998

MEMORANDUM FOR PRIVACY WORKING GROUP

FROM: TOM KALIL

There will be a meeting on Friday June 26th at 2 p.m. in Room 239 to discuss the Administration's privacy policy. The purpose of the meeting is to put together a "package" of steps that will strenghten privacy protection for consideration by NEC Deputies on July 8th.

To get cleared in for the meeting, please contact Gay Joshlyn 456-5362.

Attached are:

- A memo prepared by the Department of Commerce; and
- A description of the "privacy entity."

Distribution

Anne Reed, USDA
Peter Wathen-Dunn, ED
Becky Burr, DOC
Abel Lopez, DOE
Greg Chang, DPC
John Fanning, HHS
Jennette Smith, HUD
Scott Charney, DOJ
Roslyn Mazer, DOJ
Miriam Miller, DOL
Peggy Grafeld, DOS
Nancy McFadden, DOT
Gregory Baer, DOT
Michael Moynihan, DOT
Beverly Linden, SBA
Mark Day, EPA
Ariadne Goerke, EPA
Donald Abelson, USTR
Maya Bernstein, OMB
Jim Kohlenberger, OVP
David Beier, OVP
Tom Freedman, DPC
Mary Smith, DPC
Rebecca Blank, CEA
David Medine, FTC

MEMORANDUM

TO: Sally Katzen
Elena Kagan

FROM: Andrew Pincus

DATE: June 19, 1998

RE: Privacy Proposal

This memorandum sets forth a package of proposals for enhancing privacy protection in the information age, which follow up on the Vice President's speech on this topic last month.

I. Creation of Federal Privacy Entity

There are currently several different Executive Branch agencies that are responsible for developing, explaining and promoting the U.S. government position on privacy. For example, the U.S. Department of Commerce has taken the lead in representing the federal government position on privacy to private industry and the commercial sector generally. The Office of Management and Budget is responsible for giving Federal agencies guidance on implementation of the Federal Privacy Act, but has only occasionally addressed public audiences. A number of other government offices represent the U.S. position on privacy before our international trading partners, including NTIA/DOC, ITA/DOC, OPD/WH, and the State Department.

Given the complexity of privacy issues and the breadth of responsibility for privacy protection, we propose the creation of a Federal Privacy Entity located in the Executive Office of the President that could serve the following functions.

- *Advising* - provide experts to respond to privacy policy questions raised by government agencies (i.e., when considering legislation or drafting regulations) and private sector entities (i.e., when developing personnel practices or new information products).

- *Advocating* - monitor privacy policies that affect consumers and promote improvements through public appearances, media presence, writing to organizations about whom complaints are received, and involvement in litigation on behalf of groups and/or as amicus curiae.

- *Representation* - explain and promote U.S. government position on privacy policy domestically and internationally, advancing the Administration's privacy message, and providing coherence to Administration testimony and public position.

- *Coordination* - apprise appropriate government agencies of emerging privacy issues and ensure that the issues are addressed; ensure that the views of appropriate agencies are represented on privacy policy issues, both domestically and internationally.

- *Education* - provide privacy information to citizens, industry, and government.

II. Initiatives to Protect Specific Types of Information

The Administration already has announced its support for legislation to ensure the privacy of medical information, and the Vice President discussed this issue in his speech last month.

Recently, the Acting Comptroller of the Currency announced plans to address privacy issues with respect to personal financial information. Perhaps additional details regarding this effort could be included as part of the Administration's announcement of its privacy program.

III. Initiatives to Address Specific Activities

A. Profiling

1. Background

Profilers compile information about individuals and then sell that information. Last December, fourteen such services agreed with the FTC 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.]

2. Proposal

That the Administration seek 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, and

- giving 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.

B. Marketing of Information

1. Background

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.

2. Proposal

That the Administration propose legislation

- requiring that all persons engaged in marketing participate in a self-regulatory system with standards along the lines of the DMA principles, and
- giving 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.

C. Solicitation of Information from Children

1. Background

Solicitation of information from children raises issues different from the situation in which information is solicited from adults because children generally lack the ability to provide legally-binding consent.

2. Proposal

- propose legislation authorizing the FTC to issue rules prohibiting collection of personal information from children under 13 without prior parental consent

D. Credit Reporting

1. Background

The Fair Credit Reporting Act governs activities of credit reporting agencies that furnish reports to third parties. 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 purchase credit reports from a central bureau, but rather will obtain information directly from the individual sources. Also, the FTC is concerned that provision of the Act permitting sharing of information between "affiliates" may lead to abuses, especially as financial services companies combine.

2. Proposal

- 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.

E. State Government Data Releases

1. Background

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 laws analogous to the federal Privacy Act. 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.

2. Proposal

- 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

Then initiate discussions leading up to a privacy summit at which one or more of the following could be discussed and/or agreed to:

- States enact 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.)

F. Social Security Numbers

1. Background

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.

2. Proposal

- 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.

G. PSA Program

1. Background

Our privacy policy relies in large part on choice – an individual has the

option to protect his or her privacy. It is not clear, however, that most Americans are aware of their ability to choose.

2. Proposal

- Public Advertisement Campaign - identify 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.

- place op-eds in newspapers to inform individuals of the choices and how to effectuate them

H. Identity Theft

The Department of Justice, in conjunction with the Treasury Department, is working to formulate an Administration proposal for criminalizing identity theft.

III. Activities to Protect Privacy Online

This element will be addressed in the context of the Report to the President on the one year anniversary of the issuance of the Framework for Global Electronic Commerce.

Draft May 7, 1998 - NEC staff draft

Proposal for a privacy "entity"

Why do we need a privacy "entity"?

- Clearly, 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.

- However, privacy concerns often have to be balanced against other competing values - such as prevention of crime, prosecution of criminals, cracking down on "deadbeat dads," 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.

What kind of privacy entity do we need?

- It should be somewhere within 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 balancing competing interests, it would be better if it were located in an agency that had other responsibilities. Having an office that saw itself exclusively as a "privacy advocate" would be counter-productive.

- It should have a small staff – since the intent is to have it play a coordinating role as opposed to an operational role.

[accomodated with competing values, accomodating different interests ...]
Justice

Privacy Issues for Discussion

Categories of Information that are Potential Targets for Regulation

Medical Records

- Should the Administration endorse/formulate a particular legislative proposal?
- What can the Administration do to focus attention on the need for action and spur the legislative process?

Genetic

- Should the Administration formulate a legislative proposal along the lines of the portion of Senator Domenici's bill that restricts dissemination of genetic information (S.422)?

Biometric

- Should the Administration formulate a legislative proposal to protect biometric information?

Financial

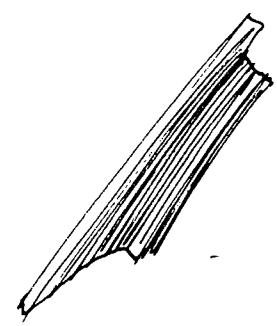
- Are there categories of financial information that should be regulated through legislation or rule?

Children

- Should the Administration propose limits on the buying and selling of information about children without the parents' consent?

Other

- Are there other categories of personal information that should be regulated?



Government Information

- Should the President issue a memorandum to agency heads or an executive order calling attention to the Administration's privacy principles as well as to the Privacy Act?

- Should agencies be directed to reevaluate their use of the "routine use" exemption in the Privacy Act?

- Do federal agencies provide sufficient protection to keep private information private? Do third parties (states and localities as well as any private parties) that receive non-public personal information from the federal government in fact maintain the confidentiality of that information? Is there a need for additional protections in the relevant MOUs or in statutes or rules?

- Information technology makes public information much more "public" than it was in the pre-electronic era, because bits of information can be combined to create a profile in a way that was not possible before. How should government respond to this new era?

  Should the Administration direct a government-wide assessment of personal data collection with the goals of (1) eliminating collection of personal data that is not necessary; and (2) ending public disclosure of personal data of identifiable individuals unless the disclosure is necessary to serve an important public purpose?

  Should some types of government information be made available only in paper form (and not in searchable databases)?

- Should the Administration challenge state and local governments to join in a dialogue to reduce the dissemination/marketing of personal information compiled by governments? Or should it propose restrictions on state governments along the lines of the Driver's Privacy Protection Act of 1994, which requires the States to allow drivers to choose whether to make their personal information available?

Profiling/Data Agglomeration

- Much profiling is facilitated by use of social security numbers as the key to bring together disparate information about an individual. Should the Administration propose tighter limits on the use of social security numbers by non-government entities?

  For example, Senator Feinstein has proposed (S.600) prohibiting the commercial sale or acquisition of an individual's social security number as well as barring its use as a personal identification number, in the absence of the individual's consent. It also might be possible to ban the transmission of social security numbers without the individuals' consent.

Even with respect to government entities, should the Administration propose a ban on the use of social security numbers in public disclosures by government entities of personal data (e.g., a state could not require use of social security numbers in connection with filing of property deeds or car registrations)?

- Can/should the government prohibit the use of government databases (or databases compiled from public records) for profiling purposes?

- Should profiling be subject to legislative/regulatory restrictions that, for example, would require the consent of the subject before personal data could be used for this purpose? Are there other appropriate restrictions?

Identity Theft

- Should the Administration formulate a legislative proposal to criminalize identity theft in some/all circumstances?

Other Measures

- We should review pending bills as well as materials issued by privacy advocates to determine whether there are other measures that should be considered.

Other Privacy Issues

Collection of Information through Internet Interactions

- In the July 1 announcement, the President stated a preference for self-regulation in this area. That policy will be reviewed on July 1, 1998, based on the progress made over the last year.

DRAFT 4/27/98

REPRESENTATIONAL FUNCTION

What is the Representational function? In performing the representational function, a federal entity would explain and promote the U.S. government position on privacy policy domestically and internationally, advancing the Administration's privacy message, and providing coherence to Administration testimony and public positions.

For what areas is there now a representational function for privacy? The Commerce Department has taken the lead in representing the federal government position on privacy to private industry and the commercial sector generally. Until it was disbanded in 1997, the Office of the Assistant to the President for Consumer Affairs fulfilled this role with respect to consumers and consumer advocacy groups. The Office of Management and Budget is responsible for giving Federal agencies guidance on implementation of the Federal Privacy Act, but has only occasionally addressed public audiences. Each of these offices has represented the government's position in testimony before Congress relevant to its constituent sector. A number of government offices represent the U.S. position on privacy before our international trading partners, including NTIA/DOC, ITA/DOC, OMB, the Office of Policy Development in the White House, and the State Department, although Commerce is most active in this role.

What were the group's thoughts on the Representation function? Participants agreed that presentation of Administration views on privacy-related policy matters to industry, to members of the public, to Congress, and to our international trading partners should be better coordinated and enhanced.

ADVISORY FUNCTION

What is the Advisory function? The advisory role is one in which experts are available to respond to privacy policy questions raised by government agencies (e.g., when considering legislation or drafting regulations) and by private sector entities (e.g., when developing personnel practices or new information products).

For what areas is there now an advisory role? The Department of Commerce is working with the private sector (commercial and public interest representatives) to develop effective self-regulation for privacy protection pursuant to the President's directive of July 1, 1997. The OMB provides guidance to federal agencies as to how to implement their responsibilities under the Privacy Act, resolves disputes among agencies about data sharing in its traditional mediating role, and responds to inquiries from the Congress about the Privacy Act when appropriate. In conducting their particular regulatory roles, other federal agencies may provide privacy policy advice to their constituents. For example, HHS provides information to health care providers and payers, and Treasury has a close relationship with the banking community.

What were the group's thoughts on the Advisory function? There seemed to be agreement that an available body of expertise is useful, and tentative agreement that an advisory function might be better coordinated and enhanced.

COORDINATION FUNCTION

What is the Coordination function? A federal privacy entity could apprise appropriate government agencies of emerging privacy issues and ensure that these issues are addressed. It could also ensure that the views of appropriate agencies are represented on privacy policy issues, both domestically and internationally.

For what areas is there now a coordination role being carried out? OMB coordinates Administration positions on legislation, testimony, and reports submitted to Congress. Otherwise, coordination is ad hoc and sporadic.

What were the group's thoughts on the Coordination function?
There was agreement that coordination is an essential function that should be significantly enhanced.

REGULATORY/ENFORCEMENT FUNCTION

What is the regulatory function? The regulatory function involves the creation and administration of legally enforceable regimes of fair information practices including the use of some combination of inspection, registration, reporting, civil or criminal action, adjudication, and penalties.

For what sectors is there now a regulatory regime for privacy? No omnibus law regulates private sector use of information. However, certain kinds of information are subject to sector-specific law. The Federal government's management of records about individuals is governed by the Privacy Act; the Office of Management and Budget is assigned in the law to prescribe guidelines and regulations and provide continuing oversight of the Act's implementation. Consumer credit information is substantially regulated by the Fair Credit Reporting Act with enforcement authority resting in the Federal Trade Commission. The banking and financial sector is governed in part by the Right to Financial Privacy Act, but enforcement is by private right of action. Student records maintained by recipients of federal funding are governed by the Family Educational Rights and Privacy Act (Buckley Amendment, FERPA). While the Department of Education does not directly regulate student records, it does advise educational institutions about their obligations under FERPA. The Electronic Communications Privacy Act as well as other wiretap statutes, governs records transmitted electronically, by telephone, electronic, or wireless communication. The Federal Communication Commission has regulatory

authority over private telephonic communications, and to the extent that these laws create criminal penalties, the law enforcement community is responsible for their implementation. There is no comprehensive national legal framework for the protection of medical records in the hands of private care providers, insurance companies, pharmacies, or manufacturers of devices or drugs, although such a framework was proposed by the Secretary of HHS on behalf of the Administration in 1997.

What were the group's thoughts on the Regulatory function? There was general agreement in the group that, consistent with the President's memorandum of July 1, 1997, a sectoral approach continues to be appropriate, and a comprehensive regulatory role across all sectors would be inappropriate.

OMBUDSMAN FUNCTION

What is the Ombudsman Role? This role involves providing case-by-case assistance to consumers or businesses in resolving in response to their particular problems or complaints. An ombudsman could act on behalf of aggrieved parties whose privacy has been unfairly or unreasonably compromised, press individual cases, and help individuals navigate the bureaucracy, either directly or by referral to an appropriate party. It could advise parties on how to resolve their disputes, or serve as decision-maker in dispute resolution.

For what sectors is there an Ombudsman now? With respect to federal information, HHS and IRS have created formal Privacy Advocates, but those offices do not have staff to handle "retail" requests. A few other agencies have offices that assist citizens, and occasionally citizens seek help from OMB, but OMB has no investigative or enforcement authority with which to assist citizens directly. No single agency has authority or resources to pursue individual cases for the government, and often individuals request assistance via Members of Congress. Although individual companies may provide ombudsmen, in general the commercial sector does not provide an administrative avenue of redress for aggrieved parties.

What were the group's thoughts on the Ombudsman function? There was general agreement that such a function, while commendable, would swamp the resources of any office that took it on in a centralized way. There was some discussion as to whether it would be appropriate for each agency to create its own Office of Consumer Affairs to assist its constituencies.

CONSUMER ADVOCACY FUNCTION

What is the Consumer Advocacy function? This role involves monitoring privacy policies that affect consumers and promoting improvements through public appearances, media presence,

writing to organizations about whom complaints are received, and involvement in litigation, either on behalf of groups that have been harmed or as *amicus curiae*.

Is there any Consumer Advocacy activity now? Within the Federal government, each agency handles its own privacy policy issues. Some agencies have created formal Privacy Advocates, such as at HHS and IRS, whose roles are, in part, to monitor and promote privacy policy within their agencies. Since the Office of Consumer Affairs was disbanded in 1997, there is no federal office whose mission is to advocate the interests of consumers in the private sector. Private sector not-for-profit privacy advocacy organizations promote the cause of consumer privacy rights in the federal government, private industry, and overseas.

What were the group's thoughts on the Consumer Advocacy function? Participants disagreed as to whether a consumer-oriented privacy advocate would be useful. The majority thought it would be viewed unfavorably by the business community and therefore counterproductive, but a few thought it had a possibility of enhancing credibility for good actors, in a manner similar to the Better Business Bureau.

EDUCATION FUNCTION

What is the Education function? The entity could provide privacy information (including model practices and "rights and responsibilities") to citizens, industry, and government. With respect to business, the entity could publicize new techniques and technologies to promote privacy as an enhanced customer service. This function would encourage consumers to learn about their rights in, and responsibilities for, their information. The entity could conduct or fund research to support this role.

What types of privacy education are going on now? In the federal sector each agency is responsible for ensuring training of agency officials who carry out the dictates of the Privacy Act or privacy-related statutes. The Legal Education Institute of the Department of Justice runs a program at least twice a year for agency attorneys and analysts on the Privacy Act in which OMB participates. The Congressional subcommittees with responsibility for privacy publish a consumers guide to the Privacy Act, and the FTC has begun more activity in the area of private sector consumer issues. Since the Office of Consumer Affairs was disbanded, however, little privacy-related education is carried out by the federal government about consumers' rights in the private sector. Some private sector public interest groups have initiated activities in this area.

What were the group's thoughts on the Education function? There seemed to be no strong feelings about this role—neither objection nor a sense of urgency. This is an area that may merit further discussion given the importance of educated consumers in creating a "market" for privacy.

EVALUATION FUNCTION

What is the Evaluation function? This function would be a policy advocacy role (as contrasted with the consumer advocacy or ombudsman roles) to give opinions, promote good ideas and practices, and scrutinize less good ones. The function would include providing technical and policy assistance at the early stages of new ideas, products, technologies, or services either upon request from a government or private sector organization, or independently. A government imprimatur on the basis of this evaluation could provide an indication of industry good actors.

Is there any Evaluation being carried out now? Where federal government programs are concerned, OMB has the authority to review new or revised systems of records (which are also published for public comment in the *Federal Register*), oversee new technology development and purchase, and promote best practices. However, due to limitations on OMB's resources, it takes an active role only for very large or visible programs. Regulated entities, such as banks or consumer reporting agencies, are reviewed by their regulating entities (e.g. Treasury. FTC), but no federal agency comprehensively evaluates private or overseas activities across sectors. Industry and advocacy groups are significantly increasing their evaluative activities.

What were the group's thoughts on the Evaluation function? The participants agreed such a role would be controversial and thought that it was unlikely to be productive. Although, in theory, issuing opinions about private sector products and services might promote good privacy practices in industry, such a function could easily evolve into a quasi-regulatory standards-setting role or be viewed as "picking winners and losers."

Department of Agriculture
Andrea Fowler
Department of Agriculture
Office of Public Affairs - Room 536A
Washington, DC 20250
202/720-8164 (voice)
202/690-1131 (fax)

Department of Commerce
Brenda Dolan
U.S. Department of Commerce
Room 6020
14th Street & Pennsylvania Avenue, NW
Washington, D.C. 20230
202-482-4115 (voice)
202-482-3270 (fax)

Judith Means
Office of General Counsel
202-482-0387 (voice)
202-205-0524 (fax)

Department of Education
Chiquitta Thomas
Privacy Act Specialist
ROB 3, Room 5624
600 Independence Ave, S.W.
Washington, D.C. 20202-4651
202-708-9265
202-708-9346 (fax)
Chiquitta_Thomas@ed.gov

*Peter Wathen-Dunn
Office of General Counsel
Division of Business and Administrative Law
202-401-6697 (voice)
202-205-0524 (fax)

*LeRoy Rooker
Family Educational Rights
and Privacy Act (student records)
202-260-3887 (voice)
202-260-9001 (fax)

Department of Energy
Abel Lopez
U.S. Department of Energy
1000 Independence Ave., S.W.
Washington, D.C. 20585
202-586-5955 (voice)
202-586-0575 (fax)

Department of Health and Human Services

Ross Cirrincione
OASPA
645F Humphrey Building
Washington, D.C. 20250
202-690-7453 (voice)
690-8320 (fax)

*John Fanning
Privacy Advocate/ASPE
202-690-5896 (voice)
202-690-5882 (fax)
jfanning@osaspe.dhhs.gov

Department of Housing and Urban Development

Jennette Smith
451 7th St., S.W.
Washington, D.C. 20410
202/708-0614 x. 3583 (voice)
202-708-3577 (fax)

Privacy Act and Law Enforcement/Investigative
Phil Kesaris
Office of Inspector General
202-708-0390 (voice)
202-708-1354

Scott Charney + Kir

Department of Justice

Stuart Frisch
General Counsel
10th and Constitution Ave., N.W.
D.C. 20530
202-514-3452 (voice)
202-514-4317 (fax)

Federal Bureau of Investigation
Kevin O'Brien
Chief, FOI and Privacy Acts Section Washington,
202-324-3625 (voice)
202-324-1695 (fax)

Office of Information and Privacy
*Kirsten Moncada
202-616-5485 (voice)
202-514-1009 (fax)

*Scott Charney
Chief, Computer Crime
514-1026 (voice)
514-6113 (fax)

Department of Labor

Miriam McD. Miller
Office of the Solicitor
200 Constitution Ave., N.W., Room S-2002
Washington, D.C. 20210
202/219-8188 (voice)
219-6896 (fax)

Department of State

Peggy (Margaret) P. Grafeld
Office of Freedom of Information, Privacy and Classificaton Review
Room 1239
Washington, D.C. 20520-1239
202-647-6620 (voice)
202-647-5159 (fax)

Department of Transportation
Diane Litman
400 Seventh St., S.W., Room 9104
Washington, D.C. 20590
202-366-9201 (voice)
202-366-7066 (fax)
diane_litman@postmaster2.dot.gov

Department of Treasury
Alana Johnson
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220
202-622-0930 (voice)
202-622-2427 (fax)
Alana.Johnson@Treas.Sprint.com
or Dale Underwood
202/622-0874 (voice)
202/622-2427 (fax)
Dale.Underwood@Treas.Sprint.com

Internal Revenue Service
*Office of the Privacy Advocate
5000 Ellin Road NCFB Rm C8300
Lanham, MD 20706
202/283-4360
202/283-4432

Disclosure of Tax Information
Chris Rizek
202-622-1338 (voice)
202-622-9260 (fax)

Small Business Administration
Beverly K. Linden
409 Third Street, S.W.
Washington, D.C. 20416
202-401-8203 (voice)
202-205-7059 (fax)

U.S. Environmental Protection Agency
Mark Day
IRM Planning and Policy Evaluation Division
401 M St., S.W., Mailcode 3404
Washington, D.C. 20460
202/260-8672 (voice)
202/401-2196 (fax)

*Ariadne Goerke
202-260-8298 (voice)
202-401-3229 (fax)
Goerke.Ariadne@epamail.epa.gov

Becky and I would like to send this out -- ok by you?

D R A F T

MEMORANDUM FOR PRIVACY CONTACTS

FROM: Bruce McConnell, OMB
Becky Burr, Department of Commerce

SUBJECT: Privacy Functions for Your Consideration

By memorandum of July 1, 1997, the President directed the Director of the Office of Management and Budget to develop recommendations on the appropriate role of government with respect to privacy protection. OMB and the Department of Commerce have been working together on this effort.

Following up on the meeting February 3, 1998, with Sally Katzen, we request your views on the attached paper discussing a variety of privacy functions that are being or could be performed by the Federal government. The paper reviews each function with respect to:

what the function consists of;

whether the function is being performed now, and, if so, by which agencies and for what sectors; and

whether the function should be continued, or started if not being done now.

The paper also sets out the group's initial views on each function, based on our discussions at the February 3 meeting.

Of course, the functions to be conducted and the placement of the office conducting them are symbiotic. Different agencies will be more or less able to perform each function. The attached paper considers only the potential functions as applied to public, private and international arenas.

The next step is to circulate the attached discussion of functions (with any necessary changes) to policy officials for their review and comment, then to integrate the results into a paper discussing what type of entity could best perform those functions selected.

Please submit comments to Maya Bernstein at OMB by electronic mail (maya@omb.eop.gov), facsimile (202/395-5167), phone (202/395-4816) by close of business Friday, March 27, 1998.

Federal Privacy Functions to Be Performed
OMB Staff Recommendation — April 24, 1998

Recommended:

Representational — Better explain and promote the U.S. government position on privacy policy domestically and internationally, advancing the Administration's privacy message, and providing coherence to Administration testimony and public positions.

Advisory — Coordinate and enhance the availability of experts to respond to privacy policy questions raised by government agencies and private sector entities.

Coordination — Apprise government agencies of emerging privacy issues and ensure that those issues are addressed. Ensure that the views of agencies are represented on privacy policy issues, both domestically and internationally.

Recommended In Part:

Consumer Advocacy — Monitor privacy policies that affect consumers and promote improvements through public appearances, media presence. *(See below for Consumer Advocacy elements not selected.)*

Education — Provide privacy information, including model practices and "rights and responsibilities" to citizens, industry and government. Publicize new techniques and technologies to promote privacy as an enhanced customer service. *(See below for Education elements not selected.)*

Not Recommended:

Regulatory/Enforcement — Create and administer legally enforceable regimes of fair information practices.

Ombudsman — Provide case-by-case assistance to consumers or businesses in resolving particular problems or complaints.

Consumer Advocacy — Write to organizations about whom complaints are received, and become involved (e.g., as *amicus curiae)* in privacy litigation.

Education — Conduct or fund research in new techniques and technologies to promote privacy.

Evaluation — Evaluate and provide a government imprimatur to new ideas, products, technologies, or services upon request.

Federal Privacy Functions to Be Performed
OMB Staff Recommendation — April 24, 1998

Recommended:

Representational — Better explain and promote the U.S. government position on privacy policy domestically and internationally, advancing the Administration's privacy message, and providing coherence to Administration testimony and public positions.

Advisory — Coordinate and enhance the availability of experts to respond to privacy policy questions raised by government agencies and private sector entities.

Coordination — Apprise government agencies of emerging privacy issues and ensure that those issues are addressed. Ensure that the views of agencies are represented on privacy policy issues, both domestically and internationally.

Recommended In Part:

Consumer Advocacy — Monitor privacy policies that affect consumers and promote improvements through public appearances, media presence. *(See below for Consumer Advocacy elements not selected.)*

Education — Provide privacy information, including model practices and "rights and responsibilities" to citizens, industry and government. Publicize new techniques and technologies to promote privacy as an enhanced customer service. *(See below for Education elements not selected.)*

Not Recommended:

Regulatory/Enforcement — Create and administer legally enforceable regimes of fair information practices.

Ombudsman — Provide case-by-case assistance to consumers or businesses in resolving particular problems or complaints.

Consumer Advocacy — Write to organizations about whom complaints are received, and become involved (e.g., as *amicus curiae)* in privacy litigation.

Education — Conduct or fund research in new techniques and technologies to promote privacy.

Evaluation — Evaluate and provide a government imprimatur to new ideas, products, technologies, or services upon request.

PRIVACY

Federal Privacy Functions to Be Performed
OMB Staff Recommendation — April 24, 1998

Recommended:

Representational — Better explain and promote the U.S. government position on privacy policy domestically and internationally, advancing the Administration's privacy message, and providing coherence to Administration testimony and public positions.

Advisory — Coordinate and enhance the availability of experts to respond to privacy policy questions raised by government agencies and private sector entities.

Coordination — Apprise government agencies of emerging privacy issues and ensure that those issues are addressed. Ensure that the views of agencies are represented on privacy policy issues, both domestically and internationally.

Recommended In Part:

Consumer Advocacy — Monitor privacy policies that affect consumers and promote improvements through public appearances, media presence. *(See below for Consumer Advocacy elements not selected.)*

Education — Provide privacy information, including model practices and "rights and responsibilities" to citizens, industry and government. Publicize new techniques and technologies to promote privacy as an enhanced customer service. *(See below for Education elements not selected.)*

Not Recommended:

Regulatory/Enforcement — Create and administer legally enforceable regimes of fair information practices.

Ombudsman — Provide case-by-case assistance to consumers or businesses in resolving particular problems or complaints.

Consumer Advocacy — Write to organizations about whom complaints are received, and become involved (e.g., as *amicus curiae)* in privacy litigation.

Education — Conduct or fund research in new techniques and technologies to promote privacy.

Evaluation — Evaluate and provide a government imprimatur to new ideas, products, technologies, or services upon request.

(PRIVACY) 4/23 — 4/24

Entity — yes | no EU

DOJ — representational | no enforcement
— advisory | ombudsman
— coordination

(HHS - agrees w/DOJ)

Worth considering
- consumer
- education

Treasury — yes | no

Coordination - but doesn't need sep. Office.

representation - not needed
NEC - Sully pushed back

regulation
ombudsman

Commerce — no need for representation.

USDA

Sully said small rep. | coordinate / advocate

MEMORANDUM

TO: **BRUCE REED, ELENA KAGAN**

FROM: **TOM FREEDMAN**
MARY SMITH
JULIE MIKUTA

RE: **INFORMATION PRIVACY**

DATE: **JULY 14, 1997**

SUMMARY

This memo summarizes a survey, reports and legislation concerning information privacy. Included are the five general privacy principles advocated by the Office of Consumer Affairs. Attached is a list of pending privacy bills, and an overview of federal laws regulating information protection.

I. CONSUMER PRIVACY SURVEY

A 1996 Survey (The Equifax/Harris Consumer Privacy Survey) of 1,005 adults found:

- 65% of respondents consider consumer privacy protection "very important" (up from 61% in 1990);
- 80% believe that consumers have lost "all control" over how personal information about them is circulated and used by companies (up from 71% in 1990);
- 67% prefer the present system of privacy protection; 28% say a federal government Privacy Commission would be best to protect the confidentiality of consumer information in the US;
- 62% (51% of Internet users, and 64% of non-Internet users) agreed "strongly" or "somewhat" that the government needs to be able to scan Internet messages and user communications in order to prevent fraud and other crimes;
- 64% of the public (71% of Internet users) disagree that service providers should be able to track the places users go on the Internet in order to send users targeted marketing offers;
- 24% say they have personally experienced a privacy invasion (25% in 1995 and 1978).

Both the 1995 and 1994 polls indicated that Americans are more concerned about privacy intrusions by government than by businesses.

II. TASK FORCE REPORTS UNDER THIS ADMINISTRATION

Since 1995, three reports have been written by task forces investigating privacy protection policy. The earliest two came from the OMB. The first developed "Privacy Principles" for information users and individuals who supply information. The second gives an overview of information protection policy and recommendations to improve it. The third, released on July 1, and written

by a task force led by Ira Magaziner, focuses on establishing a market-oriented approach to global electronic commerce. A Presidential directive to executive and agency heads requires the Secretary of Commerce and Director of the OMB to work with industry to develop privacy protection code based on the Privacy Principles.

Report of Task Force led by Ira Magaziner, "A Framework for Global Electronic Commerce" [7/1/97]

This report outlines a strategy to ensure a market-oriented approach toward commerce on the Internet. It limits the role of government to: establishing consumer and copyright protections; developing a "predictable legal environment" for electronic commerce; and negotiating international agreements on tariffs on electronic commerce. (On this last point, the report opposes any taxes/ tariffs on e-commerce.) The Vice President will oversee the implementation of these actions.

A list of directives to executive department and agency heads accompanied the release of the report. It included:

1. The Secretary of Commerce and the Director of the OMB will encourage private industry and privacy advocacy groups to develop and adopt effective rules to protect privacy on the Internet. These rules will be consistent with the Privacy Principles.

2. The Secretary of Commerce will encourage private industry to develop and adopt a filtering device that will enable Internet users to screen content not suitable for children.

3. All agencies and departments will promote efforts to make the Internet secure for e-commerce.

OMB Paper: Privacy Options [4/28/97]

This paper was written by the Privacy Working Group for the Information Policy Committee of the National Information Infrastructure Task Force. The Administrator of the Office of Information and Regulatory Affairs of the OMB chairs the Committee. The report first describes the status of electronic data protection and the Privacy Principles. It provides an overview to federal legislation concerning information privacy, and offers options on how to improve privacy protection.

<u>Recommendations for improving data protection policies</u>

The report recommends these strategies to improve privacy protection:

1. The government could formally adopt the Privacy Principles. The OMB might direct all federal agencies to incorporate the Principles in their information management and procurement practices. Congress might adopt the Privacy Principles as part of omnibus privacy legislation

2. The government could ensure that government data collection remains consistent with the Privacy Principles in the face of changing technology. The OMB's Office of Information and Regulatory Affairs has statutory responsibility with respect to the privacy legislation and could review these statutes in light of the Privacy Principles as a model for audits in the private sector. Recently, the HHS and IRS have established Privacy Advocates; this practice could be expanded to all agencies.

3. The government could play a larger role in consumer and business education. Agencies could act as "bully pulpits" to raise consumer and business awareness of this issue.

4. Government could enhance self-regulation by exploring U.S. competition law that is blamed for enforcement deficiencies with industry.

5. A federal entity with regulatory authority could be created that would drive the development of Federal data privacy policy, or oversee the various initiatives now underway.

6. A federal body without regulatory authority could be created that would: coordinate privacy policy; represent the President's views both domestically and internationally; advocate the use of fair information practices by governments and the private sector; play an advisory role in the public and/or private sector; educate consumers and businesses about privacy; involve itself in the litigation of certain cases where a citizen's or group's privacy has been unfairly invaded. The faxed Memorandum states that the Privacy Options Paper suggested the OCA could serve this function; this does not appear to be the case.

7. A non-governmental or advisory body could be created that would perform an advisory function in the public and/ or private sector.

The Privacy Principles

The same Privacy Working Group that wrote "Privacy Options" issued a set of Privacy Principles in June 1995. These are referred to in both reports described above. They are divided into three groups:

1. *General Principles*: Personal information should be acquired, disclosed and used only in ways that respect an individual's privacy. It should not be altered or destroyed, and should be accurate and relevant for the purpose for which it is provided and used.

2. *Principles for Users of Information*: Information users should assess the impact on privacy in deciding whether or not to acquire, disclose or use personal information. They should inform individuals about whom the information is being collected about why they are collecting the data, what it will be used for, how it will be handled; the consequences of providing or withholding information; and any rights of redress.

3. *Principles for Individuals who Provide Personal Information:* Individuals should be have a means to: remain anonymous when appropriate; obtain and correct their personal information; and use appropriate controls such as encryption, to protect the confidentiality and integrity of communications and transactions. (The section below on encryption and law enforcement gives information about the debate over encryption devices.) Individuals should also have an appropriate means of redress if harmed by improper disclosure or use of information.

III. THE OFFICE OF CONSUMER AFFAIRS' PRIVACY PROTECTION PRINCIPLES

These are the 5 general privacy protection principles advocated by the OCA:

1. Tell consumers, in easily understood language, when and why certain information is being collected, what's going to be done with it, and who will have access to it. Tell them how you plan to protect their privacy, and ask for feedback.

2. Collect only information applicable to the transaction at hand. Do not allow the information to be used or sold for other incompatible purposes without the individual's knowledge.

3. Provide consumers a copy of their files upon request, and make it easy for them to correct errors and use statements of explanation.

4. Allow consumers to opt in to direct marketing or other uses they feel are appropriate for the information they are providing.

5. Make a concerted effort to educate consumers generally about how information about them is gathered, analyzed, grouped into lists and rented or sold, or otherwise used.

IV. THE EUROPEAN COMMISSION

Last week, government officials (including Secretary Daley and Ira Magaziner) visited Bonn, Brussels and Asia to discuss the future of electronic commerce. Some European governments want to make Internet service providers liable for the information carried on their networks. The US approach is to let the private sector develop products that will ensure that personal information carried over networks cannot be read or tampered with. [Reuters, 7/7/97]

The European Union Data Protection Directive takes effect in the fall of 1998. It is unclear how the directive will be enforced. Under the Directive, personal data must be collected for specified and legitimate reasons and not misused. [Privacy Options Paper, p. 5]

ATTACHMENT

GENERAL PRIVACY PROTECTION PRINCIPLES

The U.S. Office of Consumer Affairs advocates five general privacy protection principles that apply across all industries. They are as follows:

1. Tell consumers, in language they can understand, when and why certain information is being collected, what's going to be done with it, and who will have access to it. Tell them how you plan to protect their privacy, and ask for their feedback on your policy.

2. Collect only that information which is germane to the transaction at hand. And do not allow the information to be used or sold for other incompatible purposes without the individual's knowledge.

3. Provide consumers a copy of their files upon request, and make it easy for them to correct errors and include statements of explanation.

4. Allow consumers to opt in to direct marketing or other uses they feel are appropriate for the information they are providing.

5. Make a concerted effort to educate consumers generally about how information about them is gathered, analyzed, grouped into lists and rented or sold, or otherwise used.

BACKGROUND PAPERS ON ADOPTING THE PRIVACY PRINCIPLES

Leslie L. Byrne

A June 2nd issue of *Time* magazine summed up the state of privacy in America by saying "snooping on your friends and neighbors has never been easier." Lining up to dish out personal information to anyone who asks or pays are a host of government agencies, credit bureaus, data collection brokers and Internet users. Little regard is given to the harm the release of this personal information could cause.

The public has a growing awareness of issues concerning privacy. Four out of five respondents to a 1995 poll conducted by Louis Harris, expressed concern about their personal privacy. By 1996, 89% of the public said they are concerned about threats to their personal privacy from both government and business. Every indication is this number is still on the rise.

There is an interesting dynamic between the government and industry wishing to encourage electronic commerce or information technology, and the misgivings the public states in these polls about privacy. It is my contention that to realize the full potential of the Internet we must give people some assurance that they have control over their own information. Similarly, to rebuild trust in government, it is imperative that the Administration state unequivocally that it is our policy to protect personal information.

We have much activity from many agencies on privacy (see DOD *Tough Cookies* editorial.) What these government efforts lack is context, an umbrella of standards that gives a government-wide guarantee on how personal privacy will be protected. The Executive Order on the Privacy Principles is such a guarantee.

Enclosed are various writings about the privacy issue. *Privacy and American Business Report* and its editor Alan Westin are generally considered pro-industry. Even with that caveat, the enclosed poll summary is very interesting.

I literally have reams more of information on this issue. I would be happy to provide additional information or answer any questions you may have.

EXECUTIVE SUMMARY of Interpretive Essay by
Dr. Alan F. Westin, Professor of Public Law & Government
Columbia University, and Academic Advisor to the Survey

My role in this essay is to explore the survey's findings from the perspectives of a political scientist who has been studying privacy issues since 1951, has been the academic advisor to two dozen national public surveys on privacy conducted by Louis Harris & Associates and Opinion Research Corporation, has been an expert witness at government hearings and a proponent of state and federal privacy protection laws, and has advised more than 100 companies and government agencies in developing innovative consumer and citizen privacy policies.

The essay puts Internet developments into a larger social perspective. It reviews some of the most important findings about computer users' privacy concerns and policy preferences; it analyzes the factors that seem to be driving these views; and, finally, it suggests the implications in this pioneer survey for all the players involved – the online industry, businesses operating on the Net, the technology community, public-interest groups, government bodies, and the individual citizens of cyberspace.

1. The Internet should be recognized as an explosive new medium where the full array of human conduct plays out, and all the traditional tensions in democratic society over individual privacy, public disclosure, and society-protecting surveillance will have to be confronted in new settings.

• As a powerful new electronic medium, the Internet is reshaping patterns of communication, information exchanges, and – potentially -- commerce. It has become a mass media preoccupation, and virtually everyone agrees that Internet development holds enormous potential for new and creative social, business, and political activity.

• But the Internet also replicates all the vices and pathologies of contemporary society, from consumer fraud and intrusive advertising to circulation of hate speech, soliciting obscene materials, promoting terrorist projects, and criminally stalking children and women. As in the earliest frontier days in America, the Internet abounds with modern-day cattlemen, sheep-herders, farmers, saloon keepers, whores, and hacker-gunmen, with the influences of the schoolmarm, minister, sheriff, and judge also struggling to be heard and felt.

• The online and Net worlds also reproduce all the basic tensions about individual privacy, public disclosure, and society-protecting surveillance that democratic societies struggle with in the off-line world — with new dangers and new opportunities just coming into focus. It is this early stage of privacy-issues development in cyberspace that the *Privacy & American Business'* online-privacy survey was designed to explore.

2. This is the first statistically representative and reliable survey that allows us to investigate the experiences, concerns, attitudes, and policy preferences on privacy issues of the 42 million adult Americans currently using the Internet. The survey also allows us to compare these privacy views with those of computer users not on the Net, and with past privacy attitudes of the general adult public.

Privacy & American Business' online-privacy survey provides 1997 data for comparing the privacy experiences, concerns, attitudes, and policy preferences of four populations:

- total adult computer users (about 100 million);
- computer users on the Internet (about 42 million);
- computer users with online services but not on the Internet (about 28 million); and
- computer users not yet online or using the Net (about 49 million)

We can also compare these orientations to the results of the survey's privacy-trend questions from the total adult public (about 190 million), based on 1995 and 1996 Harris-Westin privacy surveys. Key findings on these comparisons are:

• Demographically, computer users are younger, have more education, and higher incomes than the general public. Net users are even younger, more affluent, and better educated than computer users not on the Net.

• Computer users as a group, and the Net and online user sub-groups, share overall business-privacy concerns at the same high levels as the general public. In 1995, 80% of the total public felt that "Consumers have lost all control over how personal information about them is collected and used by companies." An identical 80% of computer users agreed with this statement in 1997, with 82% of Net users agreeing.

• On the other hand, computer users are less fearful of technology than the general public. Where 63% of the general public agreed in 1995 that "technology is almost out of control," only 55% of 1997 computer users and 36% of Net users shared that view.

• Computer and Net users are less distrustful of institutions (measured by the Harris-Westin Distrust Index) than the general public. Where the general public registered 71% in High and Medium distrust in 1995, only 60% of computer users in 1997 registered such distrust, with Net users at 56%.

• In another important overall comparison, computer users and the general public share a general preference for voluntary over regulatory policies to protect consumer privacy. If businesses and industry associations adopt good privacy protection policies, 72% of the general public said in 1995 they would prefer that approach; in 1997, 70% of computer users and 72% of Net users agreed with that view of voluntary being preferable to regulatory as

a general matter. (However, as noted below, the public often favors sector-specific legislation, when it feels problems are outpacing voluntary efforts.)

3. While only a tiny fraction of Online-Service and Net users report they have personally experienced invasions of their privacy while online, majorities of users express concern about threats to their online privacy.

• Only 5% of Net users and 7% of Online-Service users say they have personally been the victim of what they thought was an invasion of their privacy. Receiving unwanted email advertising and having personal information required or captured at web sites were the intrusions most complained of. This is a low level of direct invasion when compared to the 25% of the public that reported in 1995 that they have had their privacy invaded in the off-line world, and 35% is some particular consumer-information sectors.

• Moving from experiences to perceptions, online and Net users expressed a wide range of concerns over threats to the privacy and security of their activities online. Specifically:

-- 53% of Net users and 57% of Online-Service users say they are concerned that information about which sites they visit will be linked to their e-mail address and disclosed to some other person or organization without their knowledge or consent. Not surprisingly, 55% of Net users say the ability to choose not to give their real name is important to them in using the Internet.

-- 59% of Net users who send and receive e-mail are concerned that the contents of what they communicate will be obtained by some person or organization without their knowledge or consent.

-- 42% of those receiving unsolicited e-mail advertising say "it's getting to be a real pain" and want "to stop getting these messages." If there were a procedure for removing their e-mail addresses from unsolicited advertising, over a third (37%) of e-mail users would want their names removed from <u>all</u> solicitations. (This compares with only 17% of computer users who would remove their names from all regular postal mailings.)

-- 75% feel there are privacy problems in putting state and local government's public records with personally-identified information on the Internet , even though these are available today to anyone in manual form and organizations can buy computer tapes of such records for business, legal, and research purposes.

4. There is deep concern over web sites collecting personal information or e-mail addresses from children.

• Computer users divide about equally on whether there is a significant difference between collecting marketing information from children in the off-

line and online worlds. But, many practices generally accepted in marketing to children in the off-line world are strongly rejected for online conduct. When asked to assume that the purpose for gathering the information cited was the only use that a company would make of various types of information about children presented in a series of questions, majorities of computer users rejected the acceptability of all the types of uses presented.

• 59% of computer users say it is not acceptable to ask children for e-mail addresses for the purpose of gathering statistics on site visiting, and 58% oppose asking for such addresses to improve a business's product.

• 73% of computer users say it is not acceptable to obtain the real names and addresses of children when they register to use a site, or to purchase products.

• And, 90% say it is not acceptable (74% "not at all acceptable") for companies to rent or sell the real names and addresses of their child registrants or customers to third parties for marketing.

• 75% of computer users are NOT confident that companies on the net that are marketing to children would follow the policies they set forth on how they would handle the children's information they collect.

5. Reflecting privacy concerns, especially where children are involved, a majority of computer users say they favor legal action.

• 94% of computer users say that companies collecting information from children should be held legally liable for violations of their stated policies.

• When asked which of three roles "government" should take in approaching "Internet privacy issues," a majority – 58% – favor "passing laws NOW for how personal information can be collected and used on the Internet." 24% favor government recommending standards but not passing laws now, and 15% say government should "let groups develop voluntary privacy standards but not take any action now unless real problems arise." Only 47% of Net users favor enacting government laws now, while those computer users not using the Net or an online service favored government laws at 65%.

• It should be noted that the question on government approaches came at the end of a detailed survey exploring potential threats to privacy and security, and especially after the series on children's' privacy issues. Also to be noted is that the question did <u>not</u> specify whether state or federal governments should be the rule setters; just what kind of controls government would set, how these would be monitored, and which government agency would act as the enforcing agent; and what kinds of penalties and remedies would be installed. We can expect that the attitudes of computer users and especially

Net users would be significantly affected by the alternatives presented on those matters.

6. The views of computer users overall, and online and Net users specifically, follow some of the patterns that past privacy surveys have found to operate as driving factors in the off-line world.

• Past Harris-Westin surveys have found that two-thirds majorities of the American public (and computer users as a sub-group) oppose creation of a federal regulatory agency covering the entire private sector (as in the European data protection commissions' model). But strong majorities will favor sector-specific legislation at the state or federal levels when the perception is that serious breaches of privacy and confidentiality are taking place and voluntary controls by industry or private groups are either ineffective or not adopted widely enough. Examples have included legislation that would forbid employers or health insurers to use genetic tests for employment or underwriting purposes, and federal laws protecting privacy and confidentiality of medical records and the increased electronic movement of personally identified health information. Computer-user support for "government" action on the Net suggests that the Net is seen as a "sector" in which voluntary policies are not yet perceived as present.

• In past privacy surveys, trust in the practices of an industry in handling its customers' personal information in a "proper" or "responsible" way and "respecting its confidentiality" came through as a major factor in helping the majority of the public (our 55% "Privacy Pragmatists") to decide whether to give their personal information for organizational uses under privacy-policy promises or whether they would favor passing legislation to mandate the rules. In the 1997 online privacy survey, with ten industries that handle consumer information presented for judgment, a majority of respondents gave high ratings (in the 68-80% ranges) to employers, hospitals, banks, and companies making computer hardware and software. But online companies – those offering Online Services, direct Internet access, and marketing products on the Net – received low confidence ratings, in the low 40% levels. This placed them alongside credit bureaus and direct-mail marketers, two groups that have traditionally received low-confidence ratings in privacy surveys.

• The answers to most of the key questions relating to privacy concerns and policy preferences in our 1997 survey followed exactly the level of confidence in the three online businesses -- the lower the confidence in online firms, the more privacy-oriented the positions. This was true, for example, with all the questions involving children's privacy; concern about the confidentiality of e-mail content; concern about putting public records on the Net; desire to remove their e-mail address from all unsolicited marketing; and support for passing government laws now on Internet privacy.

7. Since 70% of computer users generally favor voluntary policies over legislative rules for consumer privacy protection, the explanations for

favoring government action now for the Internet lie in a combination of factors discussed below.

In addition to the effects of low confidence in online companies, here are factors that seem to be undercutting the traditional support for voluntary actions as of 1997:

• There has been a steady drumbeat of largely alarming stories in both the mass and online/computer media about privacy and security risks on the Internet. These often present the situation as one in which no current tools or policies are available to protect users, and that staying off the Net, not using one's credit card for purchases, and never volunteering personal information are the sensible ways to proceed. This trend is typified by the June 2, 1997 issue of Time ("No Privacy on the Net"); "Cookies a Half-Baked Idea," Inter@ctive Week, April 4, 1997; "Cyber Eyes Are Watching," Family PC, April, 1997; "What right to Privacy?," NetGuide, January 1, 1997; "Easy Now to Keep Tabs on Users' Internet Postings," N.Y. Times, January 6, 1997; "There's No Guarantee of Privacy on the Net," N.Y. Times, January 13, 1997; and "Think of Your Soul as a Market Niche," N.Y. Times, September 11, 1996. Along with movies and TV programs depicting hackers and privacy invaders trolling the Net and finding helpless victims, the media coverage has sent a message to many millions of viewers and readers that Orwell's progeny own the online world.

• Industry association policies and guidelines for collecting and using consumer information online and on the Net are in a very early stage of roll out. Most of them were developed in 1996, and the most important ones are 1997 products, some just issued in late May or early June, and some to be presented at the Federal Trade Commission's Workshop on Consumer Privacy Online in mid-June. These include policies from the Direct Marketing Association, the Interactive Services Association, and others. It is highly doubtful that respondents to our survey in April of 1997 had heard about these, or had any experiences with them with which to decide how well they worked.

• The survey recorded remarkably low awareness by online service subscribers of the information-handling policies of their current service provider. Almost three out of four online service users (71% plus 3% don't know) said they were not aware of "any rules or policies [that their] online service has as to how it will use the information it maintains or collects about [their] online usage..."

• A series of questions about how web site visitors decide whether to give registration-type information when they visit sites documented that most web site visitors are NOT today encountering clear, up-front declarations of information policy from most sites they visit. Net users say getting such information would have a major effect on their decisions whether to provide personal information, but 79% say they have declined to give information to

sites not explaining their policies, and 8% say they have given false information..

• There was also very low awareness of software tools for exercising individual control over information and communication practices.

-- 75% of e-mail users said they weren't aware of any procedure or technique to remove their e-mail address from companies or organizations sending them advertising materials.

-- 45% of parents with children using the Net said they were not aware of any software programs that let parents automatically limit the web sites their children visit or the personal information they can provide to sites.

It is also clear that very few members of the computer-using public have yet heard about new control approaches such as the e-Trust information labeling and independent-certification system for designating commercial web sites, or the privacy policies and preferences program being developed by the Center for Democracy and Technology, with strong business and public-interest group support.

Finally, strong interest was expressed by the privacy-concerned respondents in getting free and easy-to-use software tools that would allow them to state their preferences as to how they would wish their personal information to be used by business or organizational web sites, and even to conduct dialogues with such sites over just how such uses could be made acceptable. Similar strong interest was expressed by parents in getting and using software that would allow them to control what personal information their children could give to Internet sites or in chat rooms.

8. The intensity of women's concerns about privacy threats and desired protections shows up heavily in the survey results.

• Prior to 1997, within the high levels registered for the population as a whole, privacy surveys had shown women to be even more privacy concerned and regulatory-oriented than men in the off-line world. Our online survey found women widening their lead even more in the online world. Women scored 5-13 percentage points higher than men in 16 major questions here, for example:

-- 11% higher in being very concerned that sites visited could get their e-mail addresses; -- 11% higher that children's information should never be sold to third-parties;

-- 7% higher that putting public records on the Net would be a privacy problem; and

– 7% higher in saying that being able to surf the Net anonymously is very important to them.

Reflecting those gender-intensified views, women are a full 18% higher than men in saying that government should enact laws now to protect privacy on the Internet.

8. Implications for the online and Internet industries, businesses marketing online, technologists, public-interest groups, government bodies, and individual online users.

Some surveys record confusion and indecision on the part of the public on controversial issues, or such low levels of knowledge or interest that the results offer little help to the public policy-making process. This survey, I believe, is just the opposite. It offers a clear call to all the communities sharing responsibility for the unique entity that is the Internet to hear and respond effectively to the concerns of Net and online users (and also computer users not yet online) that communication, information-exchange, and consumer commerce must be made more privacy-secure than either perception or reality make it today.

The results are certainly a summons to intensified action by the online and Internet industries and all companies hoping to create broad commerce on the Net. These groups must move guidelines and policies from paper to the daily online world. They must also give strong support to the development, distribution, and effectiveness-testing of personal privacy-enhancing tools: such as personal-information-control software tools; digital signatures and biometric identifiers to assure more secure personal identification; and easy-to-use encryption programs.

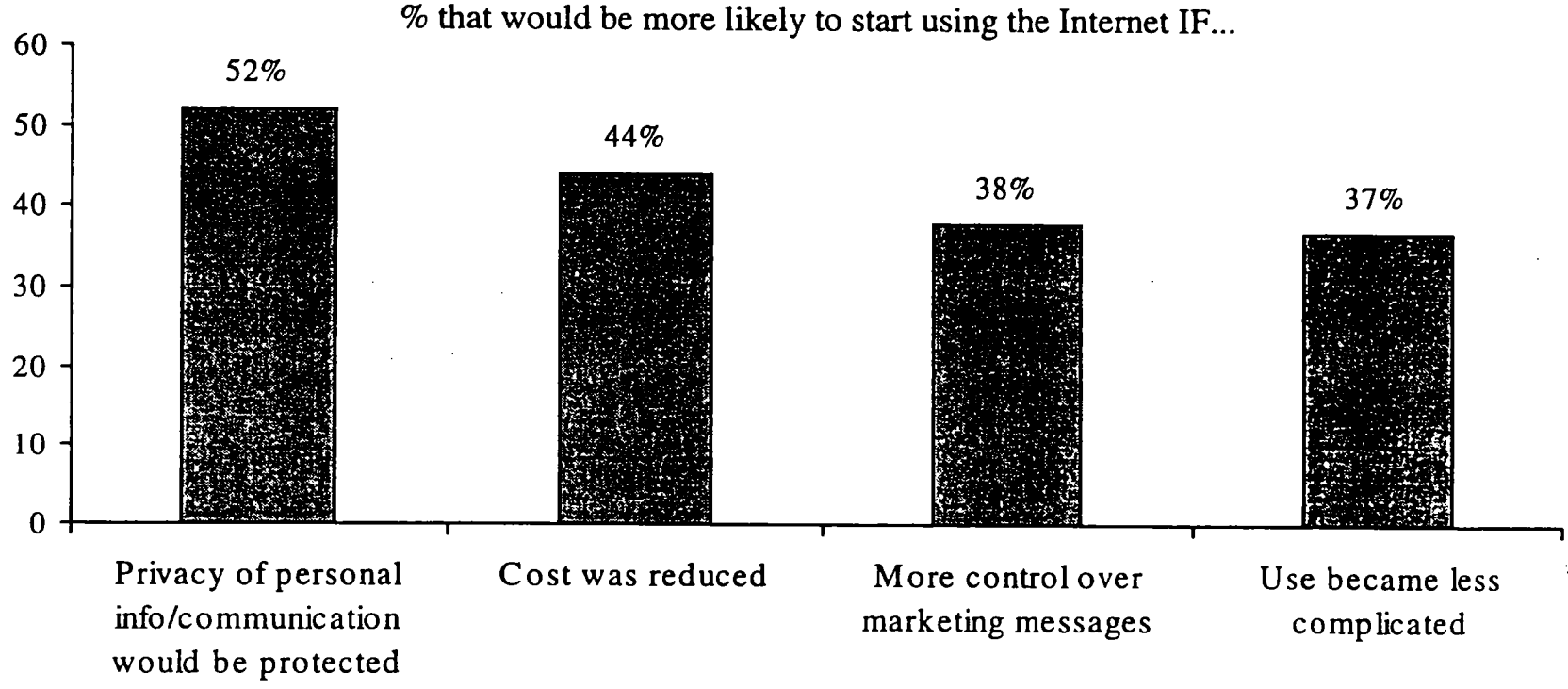
The low confidence that the survey results registered in the trustworthiness of online companies means that online business groups will have to engage in major educational programs to demonstrate that the policies and tools they support do provide an effective platform for reasonable online privacy.

If -- as this survey documents -- the growth of Internet use and especially Internet communication and commerce depend on increasing user confidence in the medium's ability to provide reasonable privacy protection, there is cause for careful optimism. When a mass market and a major societal resource of the scope of the Internet depend as much as users say it will on providing consumer and citizen confidence, the stake for business and government in making that happen is enormous.

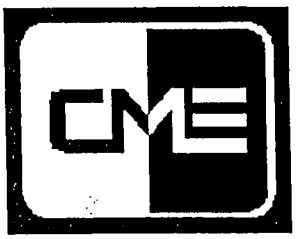
It will be fascinating to revisit these issues after two to three years, to see what progress business, government, technologists, and public interest groups will have made in bringing privacy ethics, standards, and day-to-day good practice to the Internet frontier. And, we should be able with that next snapshot to gauge what the nation's Internet users think of the privacy balances that will have been installed by that time.

Factors Increasing Likelihood of Using the Internet

Louis Harris & Associates, Inc., 1997



Base: Not very or not at all likely to start using Internet in next year (N=247)



Guidelines for the Collection and Tracking of Information from Children on the GII and in Interactive Media
Submitted to the Federal Trade Commission 1996-7

In June 1996, the Center for Media Education (CME) and Consumer Federation of America (CFA) requested that the Federal Trade Commission (FTC) issue guidelines for permissible industry practices regarding the collection and tracking of information from children on the Global Information Infrastructure and in Interactive Media. The guidelines are founded on two basic principles:

- Personally-identifiable information may be collected and/or tracked from children for commercial marketing purposes only if the collection and tracking practices are not deceptive; are fully and effectively disclosed; and valid parental consent is obtained.

- Aggregate and anonymous information may be collected and/or tracked from children for commercial marketing purposes only where the collection and tracking practices are not deceptive and are fully and effectively disclosed.

All information collectors/trackers must comply with four requirements:

1) **Disclosure must be full and effective.** The disclosure notice must include:

- what information is being collected or tracked;
- how the information is being collected or tracked;
- how the information will be used;
- who is collecting the information; and
- who will have access to the information.

These are the Privacy Principles

2) **Parental consent must be obtained.** In order for the consent to be valid:

- the child must understand that s/he needs to get parent permission before proceeding and the parent must receive complete disclosure;
- access to those areas of the site where information is collected or tracked must be conditioned on receipt of valid parental consent; and
- the burden is on the collector/tracker to obtain valid parental consent through writing or other electronic mechanisms.

3) **Parents must be able to correct information already collected about and from their children.**

4) **Parents must be able to prevent the further use of their children's information after it has been collected.**

In June 1997, at a subsequent FTC Workshop on Consumer Information Privacy, CME/CFA recommended additional guidelines regarding the collection and use of children's personally identifiable information.

All information collectors/trackers must comply with five additional requirements:

- Product spokescharacters and other mythical/fictional figures should not be used to solicit personally identifiable information from children.
- Unsolicited commercial E-mail should not be sent to children.
- Children should not be asked to release personally identifiable information about family members and other people they know.
- Free merchandise (or the chance to receive free merchandise) should not be promised to children in exchange for personally identifiable information.
- Children should not be asked to change the privacy preferences set by their parents.

For more information, contact:

Center for Media Education
1511 K Street, NW Suite 518
Washington, DC 20005
202-628-2620
www.cme/org/cme

Consumer Federation of America
1424 16th Street, NW Suite 604
Washington, DC 20036
202-387-6121

EDITORIAL

Tough cookies

Led by the Defense Technical Information Center, DOD is putting the finishing touches on a policy that would provide Web site managers with guidance on how to maintain Web logs and other electronic information gathered from visitors to its sites. This policy is expected to direct Web site managers to destroy any such electronic records after 60 days.

Recent attempts by unknown companies to gain access to the information inspired DOD to act. While the motive behind the request is unclear, the wealth of the information at stake is unmistakable. Through the use of "cookies," DOD and every other Web site host can capture information about who visits a particular site, how they entered, what files they accessed and for how long.

While we applaud DOD's decision to create a policy to protect the rights of visitors to its sites, we shudder at the possibilities of what can be done with this and similar electronic data caches. DOD officials were very upset a couple of years ago when the department discovered one of the Internet browser companies was surveying hard disks and sending information to a corporate database. We suspect DOD's primary use for the information is benign, or better still, noble in purpose: to garner information that might better serve the viewer. But do the benefits outweigh the risks?

While DOD may be the first agency to tackle the issue of Web logs and privacy, it will certainly not be the last. We believe agencies would welcome some guidance from the Office of Management and Budget as they wrestle with crafting their own policies.◀

FEDERAL Computer Week 7/7/97

MEMORANDUM

TO: TOM FREEDMAN, MARY SMITH

FROM: JULIE MIKUTA

RE: INFORMATION PRIVACY

DATE: JULY 14, 1997

SUMMARY

This memo summarizes a survey, reports and legislation concerning information privacy. Attached is a list of pending privacy bills, and an overview of federal laws regulating information protection.

I. CONSUMER PRIVACY SURVEY

A 1996 Survey (The Equifax/Harris Consumer Privacy Survey) of 1,005 adults found:

- 65% of respondents consider consumer privacy protection "very important" (up from 61% in 1990);
- 80% believe that consumers have lost "all control" over how personal information about them is circulated and used by companies (up from 71% in 1990);
- 67% prefer the present system of privacy protection; 28% say a federal government Privacy Commission would be best to protect the confidentiality of consumer information in the US;
- 62% (51% of Internet users, and 64% of non-Internet users) agreed "strongly" or "somewhat" that the government needs to be able to scan Internet messages and user communications in order to prevent fraud and other crimes;
- 64% of the public (71% of Internet users) disagree that service providers should be able to track the places users go on the Internet in order to send users targeted marketing offers;
- 24% say they have personally experienced a privacy invasion (25% in 1995 and 1978).

Both the 1995 and 1994 polls indicated that. Americans are more concerned about privacy intrusions by government than by businesses.

II. TASK FORCE REPORTS UNDER THIS ADMINISTRATION

Since 1995, three reports have been written by task forces investigating privacy protection policy. The earliest two came from the OMB. The first developed "Privacy Principles" for information users and individuals who supply information. The second gives an overview of information protection policy and recommendations to improve it. The third, released on July 1, and written by a task force led by Ira Magaziner, focuses on establishing a market-oriented approach to global electronic commerce. A Presidential directive to executive and agency heads requires the Sec of Commerce and Director of the OMB to work with industry to develop privacy

protection code based on the Privacy Principles.

Report of Task Force led by Ira Magaziner, "A Framework for Global Electronic Commerce" [7/1/97]

This report outlines a strategy to ensure a market-oriented approach toward commerce on the Internet. It limits the role of government to: establishing consumer and copyright protections; developing a "predictable legal environment" for electronic commerce; and negotiating international agreements on tariffs on electronic commerce. (On this last point, the report opposes any taxes/ tariffs on e-commerce.) The Vice President will oversee the implementation of these actions.

A list of directives to executive department and agency heads accompanied the release of the report. It included:

1. The Sec. of Commerce and the Director of the OMB will encourage private industry and privacy advocacy groups to develop and adopt effective rules to protect privacy on the Internet. These rules will be consistent with the Privacy Principles.

2. The Sec. of Commerce will encourage private industry to develop and adopt a filtering device that will enable Internet users to screen content not suitable for children.

3. All agencies and departments will promote efforts to make the Internet secure for e-commerce.

OMB Paper: Privacy Options [4/28/97]

This paper was written by the Privacy Working Group for the Information Policy Committee of the National information Infrastructure Task Force. The Administrator of the Office of Information and Regulatory Affairs of the OMB chairs the Committee. The report first describes the status of electronic data protection and the Privacy Principles. It provides an overview to federal legislation concerning information privacy, and offers options on how to improve privacy protection.

<u>Recommendations for improving data protection policies</u>

The report recommends these strategies to improve privacy protection:

1. The government could formally adopt the Privacy Principles. The OMB might direct all federal agencies to incorporate the Principles in their information management and procurement practices. Congress might adopt the Privacy Principles as part of omnibus privacy legislation

2. The government could ensure that government data collection remains consistent with the Privacy Principles in the face of changing technology. The OMB's Office of Information and Regulatory Affairs has statutory responsibility with respect to the privacy legislation and could review these statutes in light of the Privacy Principles as a model for audits in the private sector. Recently, the HHS and IRS have established Privacy Advocates; this practice

could be expanded to all agencies.

3. The government could play a larger role in consumer and business education. Agencies could act as "bully pulpits" to raise consumer and business awareness of this issue.

4. Government could enhance self-regulation by exploring U.S. competition law that is blamed for enforcement deficiencies with industry.

5. A federal entity with regulatory authority could be created that would drive the development of Federal data privacy policy, or oversee the various initiatives now underway.

6. A federal body without regulatory authority could be created that would: coordinate privacy policy; represent the President's views both domestically and internationally; advocate the use of fair information practices by governments and the private sector; play an advisory role in the public and/or private sector; educate consumers and businesses about privacy; involve itself in the litigation of certain cases where a citizen's or group's privacy has been unfairly invaded. The faxed Memorandum states that the Privacy Options Paper suggested the OCA could serve this function; this does not appear to be the case.

7. A non-governmental or advisory body could be created that would perform an advisory function in the public and/ or private sector.

The Privacy Principles

The same Privacy Working Group that wrote "Privacy Options" issued a set of Privacy Principles in June 1995. These are referred to in both reports described above. They are divided into three groups:

1. *General Principles*: Personal information should be acquired, disclosed and used only in ways that respect an individual's privacy. It should not be altered or destroyed, and should be accurate and relevant for the purpose for which it is provided and used.

2. *Principles for Users of Information*: Information users should assess the impact on privacy in deciding whether or not to acquire, disclose or use personal information. They should inform individuals about whom the information is being collected about why they are collecting the data, what it will be used for, how it will be handled; the consequences of providing or withholding information; and any rights of redress.

3. *Principles for Individuals who Provide Personal Information:* Individuals should be have a means to: remain anonymous when appropriate; obtain and correct their personal information; and use appropriate controls such as encryption, to protect the confidentiality and integrity of communications and transactions. (The section below on encryption and law enforcement gives information about the debate over encryption devices.) Individuals should also have an appropriate means of redress if harmed by improper disclosure or use of information.

III. ENCRYPTION AND LAW ENFORCEMENT

FBI Director Louis Freeh urged Congress to promote the use of a type of encryption devices that would enable law agents to access 'secured' data. [Encryption devices work by scrambling information and rendering it unreadable without a password or software "key". Freeh wants to see use of the key-type, because law agents would be able to crack the code by accessing the key.] Current law imposes tight restrictions on the export of encryption products, but domestic use is unregulated. There are four bills before Congress which address encryption.

1. Sen Leahy (S 376): to relax export controls of encryption devices and promote the use of encryption as a means of securing electronic commerce and global communications across the Internet. Computer industry supports it; Freeh and members of the Clinton administration do not.

2. Sen McCain and Sen Kerrey (S 909): to continue strict export controls of encryption without key recovery and require that all computer networks used by the federal government or funded in part by the federal government have key recovery. The Senate Commerce Committee has passed this Act; it was debated by the Judiciary Committee on 7/9.

3. Rep Goodlatte (H.R. 695-- with 165 co-sponsors): to relax export controls on encryption products

4. Rep Burns (S 377): to relax export controls, and create a Board to give law enforcement agencies special access to the development of plans for privacy enhancing technology.

IV. THE EUROPEAN COMMISSION

Last week, government officials (including Sec. Daley and Ira Magaziner) visited Bonn, Brussels and Asia to discuss the future of electronic commerce. Some European governments want to make Internet service providers liable for the information carried on their networks. The US approach is to let the private sector develop products that will ensure that personal information carried over networks cannot be read or tampered with. [Reuters, 7/7/97]

The European Union Data Protection Directive takes effect in the fall of 1998. It is unclear how the directive will be enforced. Under the Directive, personal data must be collected for specified and legitimate reasons and not misused. [Privacy Options Paper, p. 5]

DRAFT

Memorandum

Summary: Many federal agencies are working on privacy protection options (i.e. OMB, HHS, IRS and SSA etc.) Recent media accounts and many surveys highlight the public's interest in privacy issues related to government and private industry, especially as it relates to the Internet and electronic commerce. What is lacking in these efforts and interests is a context, a standard by which to measure progress. The Privacy Principles provide such a standard. Although currently voluntary, the Principles have been acknowledged by both government and industry leaders as a fair approach to the issue of protection of personal information.

Background: In his 1992 campaign material and in the recent commencement speech at Morgan State University the President highlighted the importance of protecting personal privacy in an electronic age. While there are technological tools being developed that will help enable individuals to protect their privacy, technology cannot be viewed as a panacea. There are cultural, political, and ethical questions surrounding the use and potential abuse of technology that the Administration must take into account as it develops its policies. The most recent example of resistance from the public concerning privacy and information technology is the Social Security Administration's experience with the introduction of its Personal Earnings and Benefits Statement (PEBES) on-line access. It was withdrawn in forty-eight hours after its unveiling because of public and congressional apprehension over privacy.

There is also the low tech issue of how the federal government treats individual records. This concern was recently highlighted by the disclosures of IRS employees "surfing" through individual tax records for curiosity or entertainment value. Public trust in the government's ability to secure personal information has hit an all time low.

This same "trust" issue has loomed large in the industry dialogue concerning electronic commerce. As more than one survey released during the FTC's meetings in early June noted, privacy policies of many Internet sites are nonexistent or difficult to locate. Businesses and the public alike said that the very success of the Internet as a marketplace would depend on consumer confidence in the handling of personal information.

Recommendation: The President should sign an Executive Order directing all federal agencies to incorporate the Privacy Principles in their information management and procurement practices. He should also name a privacy advocate office for the federal government. This office would act as the public's privacy ombudsman to government agencies. The OMB Privacy Options Paper suggested USOCA could serve this function. The Executive Order should also ask Congress to develop legislation that would encourage the private sector and state and local governments to adopt the Principles and to state the President's willingness to work with the international community on privacy as it applies to electronic commerce in a global marketplace.

LAWS RE: PRIVACY

The OMB report examines laws regulating the use and exchange of personal information pertaining to four areas: government records; communications; medical records; and the consumer market. These laws are summarized here.

Privacy and government records

1. *The Privacy Act of 1974*: restricts the collection, use, and dissemination of personal information by federal agencies. Federal agencies can collect personal data that is "relevant and necessary to accomplish a purpose of the agency. There is a loophole which has proven difficult to close.

2. *The Computer Matching and Privacy Protection Act of 1988*: amends the Privacy Act to close the loophole by regulating the use by federal agencies of information contained in existing agency databases.

3. *The Paperwork Reduction Act of 1980*: ensures that information being collected by a federal agency is necessary for the proper function of the agency, and requires that individual are informed about why information is being collected and how it will be used.

4. *The Freedom of Information Act*: empowers citizens to access government records, and allows agencies to not include personal information in disclosures

Communications Privacy

1. It is illegal, except in specific cases, to intercept the contents of wire, oral or electronic communications or to disclose the contents of a communication known to have been illegally intercepted. There are 2 distinctions between wire and electronic communications that have legal significance. First, electronic communications may be intercepted in connection with the suspected commission of any federal felony, but voice communications may only be intercepted in connection with certain designated offenses. Second, electronic communications are not covered by the statutory exclusionary rule, which prohibits the use of communications intercepted illegally.

2. The law also protects e-mail in storage, although storage for record keeping purposes is not covered.

3. *The Electronic Communications Protection Act (ECPA)*: prevents electronic communications service providers from disclosing information to the government unless certain conditions are met, but does not preclude them from selling that information to non-governmental entities.

4. *Other Telecommunications Services*: options like Caller ID and Automatic Number Identification (ANI) raise new privacy issues. The FCC allows callers to block their numbers from being displayed on a per-call and per-line basis. ANI enables a marketing firm to obtain the phone number of a caller and other specific personal information by using commercial

databases. This activity is not limited by any policy, and most consumers are unaware of its existence. A 1995 Dept of Commerce White Paper proposed a voluntary framework for the telecommunications industry.

5. *Self-regulations:* Online service providers are not subject to FCC regulations or federal law regulating the commercial use of information about the type, quantity and destination of a customer's use of the service. The industry has embarked on a program of self-regulation based on guidelines developed in 1995 by the Interactive Services Association. These require providers to notify subscribers of their information practices and offer customers clear, easy ways to opt out of distribution lists that are circulated to third parties.

Medical Record Privacy

Public concern about medical privacy is quite high. A 1996 Equifax Survey found that one-third of respondents consider the use of patient records without prior permission -- even when no information is released that identifies the patient -- "not at all acceptable". Fifty-seven percent found the use of patient records either somewhat or very acceptable. Medical information is shared with third parties not involved with patient care -- such as educational institutions, social welfare programs, and credit agencies; individuals are often unaware of these activities.

1. No federal statute generally protects the confidentiality of medical records in the private sector. Some health organizations and companies have voluntarily adopted privacy standards.

2. *The FTC and the Medical Information Bureau* (MIB) have developed an agreement whereby insurance companies must notify customers when insurance companies deny them coverage or charge a higher rate based on information obtained by the MIB.

3. *Health Insurance Portability and Accountability Act (HIPAA)* in 1996: encourages development of a health information system based on uniform technological standards for electronic transmission of financial and administrative health care data; and requires the Sec. of HHS to submit recommendations to Congress with respect to the privacy of individually identifiable health information by Aug, 1997.

Consumer Market Privacy

1. *Personal Financial Records*: Banks, the government and credit reporting agencies possess detailed information on the financial status of individuals. The use and disclosure of this information is not entirely regulated. For example, "information brokers" that create databases or personal information are essentially unregulated. Some financial institutions have adopted privacy policies. Some credit reporting agencies have also adopted voluntary privacy standards. Some of these standards will become mandatory under the changes Congress has made to the Fair Credit Reporting Act of 1996 (the changes go into effect this October).

2. *Direct Marketing*: Databases built on information obtained through purchases made through the mail are not subject to laws prohibiting the use of the information for purposes other than

the original marketing activity. Individuals have no legally enforceable right to be notified when marketing data is collected, who has it, who organizes it, and with whom it is shared. The Direct Marketing Association encourages its members to adopt guidelines regulating the use of personal date, but this has not stopped the flow of unsolicited mail and telephone calls.

3. *FTC's activities*: The FTC's Bureau of Consumer Protection undertook a Consumer Privacy Initiative in 1995 to educate consumers and businesses about the use of personal information online.

Critics of the U.S.'s privacy protection policies

These are the concerns of the critics of U.S. data protection policy:

1. Privacy rules are made on a piece-meal basis, and differ from sector to sector. This makes it difficult for consumers to anticipate how their personal information will be used. Supporters argue that a sectoral approach is more likely to be effective than a single overarching policy.

2. Self-regulatory efforts of industry are laudable, but not enforceable.

3. There is no single federal agency which co-ordinates and lobbies for privacy initiatives.

The Equifax / Harris Consumer Privacy Surveys

1996 Equifax/Harris Consumer Privacy Survey

Executive Summary

---

1. Nearly two thirds of the public (65%) say "protecting the privacy of consumer information" is "very" important to them. This figure represents a significant four-point increase since 1995 when 61% expressed a similar feeling.

- Although privacy is obviously important to a majority of the public, it is not the most important. "Controlling the cost of medical insurance" and "staying out of excessive debt," for example, are "very" important to 87% of the public.

- More than three in four people (76%) say "reducing insurance fraud" is "very" important to them and 67% say the same of "controlling false advertising."

2. By a margin of two to one the public identifies actual experiences (either directly or indirectly) versus what they see or hear in the media as having the most influence on how they view business practices.

- Nearly one in two people (49%) say their "own personal experiences" have the greatest influence on their attitudes about whether businesses today are handling personal consumer data in a proper way and another 17% say "the experiences of their friends" have had the greatest influence.

- Nearly a third (32%) say "the media" have the most influence on their attitudes toward business practices.

3. The number of people who say they have been the victim of what they felt was an improper invasion of privacy remains virtually unchanged since 1991.

- Today one in four people (24%) say they have personally experienced a privacy invasion. The figure was 25% in both 1995 and 1991, and 19% in 1978.

4. Recent survey figures suggest that the public may be becoming more optimistic in their outlook toward privacy protection in the year 2000.

- In 1992, more than half of the public (55%) predicted that privacy protection in the year 2000 would get worse and only 12% thought it would get better. By 1995 only 41% of the public thought privacy protection would get worse and only 44% think so today.

- Along with the drop in pessimism is a slight increase in optimism. In 1992, 12% of the public predicted privacy protection would get better. That figure increased to 16% in 1995 and is at 17% today.

5. By a margin of two to one, the public expresses a preference for the present system of privacy protection over a federal government Privacy Commission.

- Compared to the 67% who say they would prefer the present system, only 28% say a federal government Privacy Commission would be best to protect the confidentiality of consumer information in the U.S.

- The preference for the present system is also evident among a majority of privacy pessimists (63%) (i.e., those people who predict that privacy protection will get worse in the year 2000).

6. More than half the public feel it is very acceptable for businesses to use criminal record and motor vehicle information to help combat fraud. They are less enthusiastic, however, about letting businesses have access to medically-related information.

- Among a list of six types of information, the type of information that appears to be most acceptable for use in preventing fraud and abuse is "criminal record information regarding an applicant's conviction for fraud" with 60% of the public indicating it would be "very" acceptable if businesses were to access this information in order to combat insurance fraud.

- More than half (51%) also say it would be "very" acceptable to access "motor vehicle records to identify an applicant's dangerous driving history."

- No more than four in ten people, however, feel it would be "very" acceptable to use "workers compensation data to verify an applicant's previous injuries or disabilities" (40%), or "health claims data to verify information the applicant supplied on an insurance application" (36%), or "medical records to verify any history of diseases, illnesses, and injuries asked about on the application" (31%).

- The type of information the public seems most protective of is "pharmaceutical data to identify prescriptions the applicant is taking for medical conditions not listed on the application." Only 25% of the public feel it is "very" acceptable for businesses to use this information, while 26% feel it is "not at all" acceptable.

7. More than half of the public would find the practice of using their patient records for research at least "somewhat" acceptable, though only one in five would find this "very" acceptable.

- Overall, 57% of the public would find the use of their patient records in medical research either "very" (18%) or "somewhat" (39%) acceptable.

- Nearly one third (31%) say such use of their medical records would be "not at all" acceptable.

8. Judging by their anticipation of negative effects if businesses were not able to access credit reports, the majority of people appear to recognize the benefits that these reports provide to consumers.

- Leading the list of five consequences of the inability to obtain credit reports is an "increase in the cost of credit to cover increases in bad debt" an outcome that 47% of the public think would be "very likely" to happen and another 44% think "probably" would happen.

- Other outcomes considered "very likely" to happen include: "many businesses [asking for loans] to be secured" (42%), "many businesses [cutting] back on extending credit, to only the best customers" (34%), and "[taking] several weeks rather than several days to get a loan approved" (31%).

- One in four (26%) also think that "people with good credit records would not get the lower costs that their records deserve" if accurate and relevant consumer credit reports were not available.

9. Most people appear to accept businesses' use of formulas from credit reporting companies that help to identify customers whose debt levels and spending patterns strongly suggest they will go bankrupt or become seriously delinquent.

- One quarter of the public (24%) say the use of formulas from credit reporting agencies to assess the likelihood of bankruptcy is "very" fair.

- The majority of the public (55%) think the use of bankruptcy formulas is "somewhat" fair.

10. At least half of the public express interest in on-line services related to obtaining credit reports and health-related information. Not surprisingly, the biggest predictor of interest is not simply computer use, but use of on-line services and the Internet.

- Overall, 22% of the public would be "very" interested in a computer-based on-line service that would let them identify themselves with a special password, in order to receive on-line their latest credit report and another 29% would be "somewhat" interested. One third of on-line service users (33%) and 35% of Internet users say they would be "very" interested in such a service (compared to 19% of non-on-line service users and 18% of non-Internet users).

- Half of the public (50%) say they would be interested in an on-line computer service providing information to choose physicians, hospitals, and health plans 16% say they would be "very" interested and 34% say they would be "somewhat" interested. Computer users (17%) especially those who use on-line services (25%) or access the Internet (24%) show greater interest than non-computer users (15%, 14%, and 14%, respectively, say they are "very" interested).

- Overall, 17% of the public say they would be "very" interested in accessing health and wellness educational information on-line, and another 34% would be "somewhat" interested. On-line service users (25%), and people who access the Internet (24%) are among those most likely to say they would be "very" interested in the service.

11. Public opinion is divided regarding privacy protection on the Internet, with Internet users leaning toward greater privacy protection and less intervention on the part of the government.

- Nearly half of the public agree that users should be able to visit Internet sites and use e-mail without having to give their real identities 21% agree "strongly," 27% agree "somewhat," and half disagree, with 21% disagreeing "somewhat" and 29% disagreeing "strongly." Among Internet users, however, the majority agree that this anonymity should exist 30% agree "strongly" and another 30% agree "somewhat."

- When it comes to whether the government needs to be able to scan Internet messages and user communications in order to prevent fraud and other crimes, the public leans toward agreement with 32% agreeing "strongly" and 30% agreeing "somewhat." A difference of opinion is revealed, however, when Internet users are compared with non-users only 51% of Internet users agree that the government should be able to do this compared to 64% of non-users who think so.

- The majority of the public (64%) disagree that providers of on-line services should be able to track the places users go on the Internet in order to send these users targeted marketing offers. An even greater proportion of Internet users (71%) disagree with 43% of them disagreeing "strongly."

12. The public appears to have made a notable shift over the past few years in how they regard mail offers received at their homes. Compared to 1991 and 1994 when nearly half of the public said they regard mail offers as a nuisance (46% and 47% respectively), less than four in ten (37%) say they feel that way today.

- Complementing this finding is the increase in the percentage of people who say they rarely use mail offers but do not see them as a problem (38% felt this way in 1991, and 35% in 1994 compared to 43% who feel this way today).

- There has also been a gradual but steady increase in the percentage of people who regard mail offers at their homes as a useful opportunity (6% felt this way in 1991, 10% in 1994, and 12% in 1996).

- Only 7% of the public currently regard mail offers sent to their home as invasions of privacy. (In 1991 this figure was 9%; in 1994 it was 7%.)

13. The percentage of people who report being aware of any procedures that allow one to remove one's name from direct mail lists for catalogs, products, and services has remained constant from 1991 to the present at 44%.

- The people most likely to report being aware of the procedures to have names removed from direct mail lists are the same people most likely to have ordered something in the past year. Overall, 52% of those who say they have ordered something in the past year also say they are aware of the procedures (v. 33% among those who have not ordered something in the past year).

- Notably, only 29% of those people who consider mail offers an invasion of privacy are aware of the procedures that would allow them to remove their names from direct mail lists.

14. If a procedure were available to have one's name removed from all mailing lists, some mailing lists, or no mailing lists, three out of four people (73%) would elect to have their names removed from only some lists.

- Assuming such a procedure were available, only 15% say they would have their names removed from all lists, while only 12% say they would have their names removed from no lists.

- The corresponding figures in 1991 were 64% (for some lists), 22% (for all lists), and 13% (for no lists), demonstrating an increased desire to receive at least some direct mailings.

- Even among the groups of people who have: experienced invasions of privacy, think of mail offers as invasions of privacy, think of mail offers as a nuisance, and who have not ordered in the past year majorities would still want to keep their names on some direct mail lists (69%, 64%, 73%, and 64%, respectively).

15. Most people feel the practice of compiling profiles of individual consumers' purchasing patterns and using this information to mail offers of goods and services to consumers who appear likely to be interested in these products is at least "somewhat" acceptable (66%); 11% feel it is "very" acceptable; 55% say it is "somewhat" acceptable.

- Not surprisingly, the greatest support for purchase pattern profiling comes from people who feel mail offers are useful opportunities (24% v. 14% or less among people who do not view mail offers this way).

- In contrast, 47% of the people who regard mail offers as invasions of privacy say that that consumer purchase pattern profiling is "not at all" acceptable.

16. Just over half the public would find the practice of sending pre-approved offers of insurance by mail "very" or "somewhat" acceptable when it comes to offers of automobile and other property insurance (52%) and life insurance (51%).

- More than one in four, however, would find this practice "not at all" acceptable (26% for auto/property and 27% for life).

- The figures do not change significantly when people are asked about the acceptability of using credit report information in order to qualify consumers for these pre-approved offers. With regard to auto and other property insurance, 55% of the public would find this practice "very" or "somewhat" acceptable. For life insurance, the corresponding figure is 45%.

- When people are told that consumers who are not interested in receiving these pre-approved offers of insurance could have their names and addresses removed from these mailing lists, the percentage of people overall who would find it acceptable to use credit report information to qualify consumers for these pre-approved offers reaches 90% for automobile or other property insurance and 88% for life insurance.

Survey Contents Page | **Consumer Center** | **Equifax Home Page**

individual's seclusion or solitude, or into his private affairs; public disclosure of embarrassing private facts about the individual; publicity that places the individual in a false light in the public eye; and appropriation, for another person's advantage, of the individual's name or likeness. *Id.*

19. *See* 381 U.S. 479 (1965).

20. *See, e.g.,* Minister of Supplies and Services, Industry Canada, Privacy and the Canadian Information Highway, Cat. No. C2-229/1-1994 (1994).

21. Alan Westin, Privacy and Freedom 7 (1976). *See also,* Alan Westin, The Equifax Report on Consumers in the Information Age XVIII (1990).

22. *See* Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697, 12 U.S.C. §§ 3401-22 (1994); Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1127 *as amended by* Omnibus Consolidated Appropriations Act for Fiscal Year 1997, Pub. L. No. 104-208, div. A, tit. II, § 2402(a)-(g), 110 Stat. 3009 -____, 15 U.S.C.A. § 1681-1681u (1986 & Supp. 1997).

23. For example, the Morris Worm (a harmful, replicating computer program inserted into the Internet in 1988), was designed not to be traceable to its source, and shut down thousands of computers in one day. *See* Katie Hafner & John Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier (1991).

1005 telephone interviews - 7/20-29/96 adult

24. *See generally,* Louis Harris And Associates, Inc., The 1996 Equifax/Harris Consumer Privacy Survey (hereinafter 1996 Equifax Survey) (1996). Sixty-five per cent of the participants consider consumer privacy protection "very important," up from 61% in 1995. Threats to personal privacy concerned 64% of the respondents in 1978, 79% in 1990 and 1993, 82% in 1995 and 87% in 1996. In 1990, 71% said they believed consumers had lost "all control" over how personal information about them is circulated and used by companies. By 1995 that number rose to 80%. Likewise, in 1990, 42% indicated that they have refused to give information to a business or company that they thought was either not needed or too personal. By 1995, that number rose to 59%. Of those surveyed in the 1995 poll, however, 17% agreed "strongly" and 40% agreed "somewhat" that businesses handling personal information were paying more attention to privacy issues. Both the 1995 and 1994 polls indicated that Americans remain more concerned about privacy intrusions by government than by businesses.

25. One data management and marketing company maintains approximately 350 terabytes of information about consumers (one terabyte being equivalent to 500 million pages of single-spaced text). *See* Elisa Williams, *Mining for Megadata: Mountains of Customer Information are Constantly Being Formed and Tapped,* Orange County Reg. (Calif.), Apr. 22, 1996, at D23, *available in* 1996 WL 7023685.

26. Three examples illustrate the point:

(1) Recipients of an "800" or "900" number call can identify the caller's number through Automatic Number Identification (ANI), use a reverse directory to obtain the caller's address, and compile this information into a computerized list that can be sold to other marketers. *See* Peter Sinton, *Perils Await the Unwary on the Cyber-Frontier,* S. F. Chron., Feb. 7, 1995, D10, *available in* 1995 WL 5262597; Connie Koenenn, *How they Get Your Number - From You,* Chi. Sun-Times, Sept. 15, 1993, at 37, *available in* 1993 WL 6549139.

(2) Individuals who attend a hospital sponsored seminar, health fair, or health screening may be placed on a

Presidential Advisor Ira Magaziner Briefs Council on E-Commerce Proposals

Briefing Notes

President Clinton is planning a White House event for July 1 to release the Administration's final version of its **"Framework for Global Electronic Commerce,"** a white paper on proposals dealing with regulation of the Internet and Internet commerce. Participating from the Cabinet will be Treasury Secretary Robert Rubin, Commerce Secretary William Daley, and US Trade Representative Charlene Barshefsky, among others. The White House also hopes to draw participants from both industry and state and local government.

Following the July 1 unveiling of the white paper, different cabinet secretaries will take responsibilities for implementing the new proposals. Secretaries Rubin and Daley and Trade Representative Barshefsky will be taking the paper to foreign capitals to seek international support.

The Administration currently is working on Version 16 of the **Framework.** Magaziner described the following principles that will be integral to the White House proposals:

(1) Electronic commerce on the Internet has enormous potential, affecting up to 25 percent of the total economy -- consulting, software, data transfers, real estate, retailing, etc.

(2) The Administration considered two models -- a regulatory model based on the telecommunications industry and a free-market approach, and decided to pursue the free-market option. The private sector should lead in the development of electronic commerce, Magaziner said, by setting industry standards. Under the White House proposals, private buyers and sellers will be able to come together freely in a largely unregulated environment.

(3) The US government and other governments should have minimal involvement in the development of electronic commerce and the Internet. Government intervention should be limited to safeguarding legal issues (i.e., protecting intellectual property rights).

(4) The white paper focuses on the unique nature of the Internet -- developing technology and business practices should be flexible.

(5) Because the Internet is a global endeavor, there should be international agreement on how the Internet and electronic commerce will develop. The White House will be spreading this message to its international trading partners, urging a minimum of government intervention in the future.

In answer to specific questions from state legislators, Magaziner said:

(1) The Administration is finalizing encryption proposals, and believes that the encryption key should be administered by independent third parties.

(2) Protecting privacy of information on the Internet is a primary goal of the white paper.

(3) The White House continues to explore how to protect children from "Internet

indecency." The White House will stress empowering parents to deal with these issues, either through simple options in Internet agreements with providers or through browser software that will allow them to use either rating systems or filtering choices to keep children out of objectionable Internet sites.

(4) Commerce Secretary Daley will be charged with establishing uniform standards for digital signatures.

(5) The White House is continuing to monitor whether there is a possibility for the creation of "monopolistic" Internet providers. As an example, Magaziner mentioned the task of assigning domain names (currently 100,000 domain names are registered globally ***each week***).

(6) The White House will use its international meetings to encourage trading partners not to set up special content rules that could be considered non-tariff trade barriers.

(7) Magaziner said the White House supports the broad policy goals of the Cox-Wyden bill that would place a moratorium on taxation specific to the Internet. He gave several examples of White House thinking on the issue:

> (a) The Administration opposes any new tax on the Internet in the short term, and believes that any tax on the Internet should be uniform, simple, and tax-neutral.
>
> (b) If a new tax is developed, it should be developed in a system that allows all the states to meet and set up a uniform system of taxation.
>
> (c) Internet operations should allow for the duty-free transfer of products and services in appropriate circumstances. (Magaziner said that if the order and delivery both occur on-line, then there should be no duty and no tax; if the order occurs on-line with mail or other delivery, then there is no way to avoid a duty on overseas transactions and the operation may be subject to sales or use taxes domestically).

Return to USIC home
Return to USIC FAQ page

The Privacy Working Group has recently issued the final version of its Principles for Providing and Using Personal Information. Comments and questions should be referred to Jerry Gates, Chair of the Working Group at ggates@info.census.gov.

PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE:

PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION

Privacy Working Group

Information Policy Committee

Information Infrastructure Task Force

Final Version

June 6, 1995

INTRODUCTION

The National Information Infrastructure ("NII"), with its promise of a seamless web of communications networks, computers, databases, and consumer electronics, heralds the arrival of the information age. The ability to acquire, process, send, and store information at an acceptable cost has never been greater, and continuing advances in computer and telecommunications technologies will result in ever-increasing creation, use, and storage of information.

The NII promises enormous benefits. To name just a few, the NII offers the possibilities of greater citizen participation in deliberative democracy, advances in medical treatment and research, and quick verification of critical information such as a gun purchaser's criminal record. These benefits, however, do not come without a cost: the loss of privacy. Privacy in this context means "information privacy," an individual's claim to control the terms under which personal information--information identifiable to an individual--is acquired, disclosed, and used.

Two converging trends--one social, the other technological--lead to an increased risk to privacy in the evolving NII. As a social trend, individuals will use the NII to communicate, order goods and services, and obtain information. But, unlike paying cash to buy a magazine, using the NII for such purposes will generate data documenting the transaction that can be easily stored, retrieved, analyzed, and reused. Indeed, NII transactional data may reveal who communicated with whom, when, and for how long, as well as who bought what, for what price. Significantly, this type of personal information is automatically generated, in electronic form, and is therefore especially inexpensive to store and process.

The technological trend is that the capabilities of hardware, software, and communications networks are continually increasing, while costs are continually decreasing, allowing information to be used in ways that were previously impossible or economically impractical. For example, before the NII, in order to build a profile of an individual who had lived in various states, one would have to travel from state to state and search public records for information about the individual. This process would have required filling out forms, paying fees, and waiting in line for record searches at local, state, and federal agencies, such as the departments of motor vehicles, deed record offices, electoral commissions, and county record offices. Although one could manually compile a personal profile in this manner, it would be a time-consuming and costly exercise, one that would not be undertaken unless the offsetting rewards were considerable. In sharp contrast, today, as more and more personal information appears on-line, such a profile can be built in a matter of minutes, at minimal cost.

These two converging trends guarantee that as the NII evolves, more personal information will be generated and more will be done with that information. Here lies the increased risk to privacy. This risk must be addressed both to secure the value of privacy for individuals and society and to ensure that the NII will achieve its full potential. Unless this is done, individuals may not participate in the NII for fear that the costs to their privacy will outweigh the benefits. The adoption of principles of fair information

practice is a critical first step in addressing this concern.

While guidance can be found in existing laws and principles, these need to be adapted to accommodate the evolving information environment. This changing environment presents new concerns.

* No longer do governments alone acquire and use large amounts of personal information; the private sector now rivals the government in acquiring and using personal information. New principles would thus be incomplete unless they applied to both the governmental and private sectors.

* The NII promises true interactivity. Individuals will become active participants who will create volumes of data containing the content of communications as well as transactional data.

* The transport vehicles for personal information--the networks--are vulnerable to abuse; thus, the security of the network itself is critical to the NII's future success.

* The rapidly evolving information environment makes it difficult at times to know how to apply traditional ethical rules, even ones that are well understood and accepted when dealing with tangible records and documents. Consider, for example, how an individual who would never trespass into someone's home might rationalize cracking into someone's computer as an intellectual exercise. In addition, today's information environment may present questions about the use of personal information that traditional rules do not even address.

These "Principles for Providing and Using Personal Information" ("the Principles") are offered to respond to this new information environment. The Principles attempt to provide meaningful guidance, striking a balance between abstract concepts and a detailed code. They are intended to guide all NII participants and should be used by those who are drafting laws and regulations, creating industry codes of fair information practices, and designing private sector and government programs that use personal information.

The limitations inherent in any such principles must be recognized. The Principles do not have the force of law and do not create any substantive or procedural right enforceable at law. They are not designed to produce specific answers to all possible questions; nor to single-handedly govern the various sectors that use personal information. The Principles should be interpreted and applied as a whole, pragmatically and reasonably. For example, those applying these principles should consider:

* the benefits to society from the use of personal information, recognizing that privacy interests are not absolute and must be balanced by the need for legal accountability, adherence to the First Amendment, law enforcement needs, and other societal benefits recognized in law;

* the extent to which the decision to provide personal information is voluntary, and the individual's expectations regarding the use of the information (taking into account the notice and the scope of consent provided);

* the sensitivity of the information and the potential for harm to the individual that could result from a particular disclosure or use of the information;

* the cost and effort required to protect against harm to individuals, recognizing that more sensitive information may require more costly and elaborate protection procedures than less sensitive information.

Where an overly mechanical application of the Principles would be particularly unwarranted, phrases with the words "appropriate" or "reasonable" appear in the text. This flexibility, built into the Principles to address hard or unexpected cases, does not mean that the Principles need not be adhered to rigorously. Finally, the Principles are intended to be consistent with the spirit of current international guidelines, such as the OECD Guidelines,/1/ regarding the use of personal information. The Principles invite further international cooperation over the development and harmonization of global privacy policies, adherence to which will bolster the ongoing development of the Global Information Infrastructure.

PREAMBLE

The United States is committed to building a National Information Infrastructure ("NII") to meet the information needs of its people. This infrastructure, created by advances in technology, is expanding the level of interactivity, enhancing communication, and allowing easier access to services. As a result, many more users are discovering new, previously unimagined ways to acquire and use personal information. In this environment, we are challenged to develop new principles to guide all NII participants in the fair use of personal information.

Existing codes of fair information practice must be adapted to a new environment in which information and communications are sent and received over networks by users who have very different capabilities, objectives, and perspectives. In this interactive, networked environment, many new relationships are being formed among individuals, communication providers, and other NII participants. New principles must acknowledge that each party has a different relationship with the individual and has different uses for personal information.

New principles should not diminish existing constitutional and statutory limitations on access to information, communications, and transactions, such as requirements for warrants and subpoenas. Such principles should ensure that access limitations keep pace with technological developments. These principles should acknowledge that all elements of our society share responsibility for ensuring the fair treatment of individuals in the use of personal information, whether on paper or in electronic form. Moreover, the principles should recognize that the interactive nature of the NII can empower individuals to participate in protecting information about themselves. The new principles should also make clear that this responsibility can be exercised only with openness about the process, a commitment to fairness and accountability, and continued attention to security. Finally, the principles should recognize the need to educate all participants about the new information infrastructure and how it will affect their lives.

These "Principles for Providing and Using Personal Information" ("the Principles") recognize the changing roles of government and industry in information acquisition and use. Thus, they are intended to apply to both public and private entities. The Principles are designed to guide all NII participants as well as those who are drafting legislation and crafting policy regarding the use of personal information. They provide the basic framework from which specialized principles can be developed as needed.

Trade-offs will be inevitable in implementing the Principles because privacy interests are not absolute and must be balanced against the need for accountability, the value of an unabridged flow of information, and other societal benefits recognized in law, such as lawful law enforcement activities. For example, certain decisions about the flow of personal information have already been made for us by the First Amendment, and nothing in the Principles should be read to require policies derogating the constitutionally protected freedom of speech and the press. Given these sometimes conflicting interests and public policies, the Principles must be implemented pragmatically yet conscientiously, giving due consideration to issues such as the extent to which providing personal information is voluntary, the adequacy of the notice regarding how the personal information may be used, the scope of the individual's consent, and the cost of protecting information in light of the information's sensitivity.

PRINCIPLES AND COMMENTARY

I. General Principles for All NII Participants

1. Three fundamental principles should guide all NII participants. These three principles--information privacy, information integrity, and information quality--identify the fundamental requirements necessary for the proper use of personal information, and in turn the successful implementation of the NII. All NII participants should use appropriate means to ensure that these principles are satisfied.

I.A. Information Privacy Principle

Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.

2. The NII can flourish only if all participants respect information privacy. Information privacy is an

individual's claim to control the terms under which personal information--information identifiable to an individual--is acquired, disclosed, and used. The level of privacy that must be respected is an individual's reasonable expectation, an expectation subjectively held by the individual and deemed objectively reasonable by society. Not all subjectively held expectations will be honored as reasonable. For example, an individual who posts an unencrypted personal message on a bulletin board for public postings cannot reasonably expect that personal message to be read only by the addressee.

3. What counts as a reasonable expectation of privacy under the Principles is not limited by what counts as a reasonable expectation of privacy under the Fourth Amendment of the United States Constitution. In many instances, society has deemed it reasonable to protect privacy at a level higher than that required by the Fourth Amendment. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988); Right to Financial Privacy Act, 12 U.S.C. § 3401 (1988); Privacy Act, 5 U.S.C. § 552a (1988). The Information Privacy Principle fully supports such possibilities.

4. As explained in later principles and commentary, an individual's privacy can often be best respected when individuals and information users come to some mutually agreeable understanding of how personal information will be acquired, disclosed, and used. However, in certain cases--for example, if the individual lacks sufficient bargaining power--purely contractual arrangements between individuals and information users may fail to respect privacy adequately. In such instances, society should ensure privacy at some basic level in order to satisfy the Information Privacy Principle.

I.B. Information Integrity Principle

Personal information should not be improperly altered or destroyed.

5. NII participants should be able to rely on the integrity of the personal information the NII contains. Thus, personal information should be protected against improper alteration or destruction.

I.C. Information Quality Principle

Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

6. Personal information should have sufficient quality to be relied upon. This means that personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

II. Principles for Users of Personal Information

II.A. Acquisition Principles

Information users should:

1. Assess the impact on privacy in deciding whether to acquire, disclose, or use personal information.

2. Acquire and keep only information reasonably expected to support current or planned activities.

7. The benefit of information lies in its use, but therein lies an often unconsidered cost: the threat to information privacy. A critical characteristic of privacy is that once it is lost, it can rarely be restored. Consider, for example, the extent to which the inappropriate release of sensitive medical information could ever be rectified by public apology.

8. Given this characteristic, privacy should not be addressed as a mere afterthought, once personal information has been acquired. Rather, information users should explicitly consider the impact on privacy in the very process of designing information systems and in deciding whether to acquire or use personal information in the first place. In assessing this impact, information users should gauge not just

the effect their activities may have on the individuals about whom personal information is acquired, disclosed, and used; they should also consider other factors, such as public opinion and market forces, that may provide guidance on the appropriateness of any given activity.

9. After assessing the impact on information privacy, an information user may conclude that it is appropriate to acquire personal information in pursuit of a current or planned activity. A planned activity is one that is contemplated by the information user, with the intent to pursue such activity in the future. In all cases, the information user should acquire only that information reasonably expected to support those activities. Although information storage costs decrease continually, it is inappropriate to collect volumes of personal information simply because some of the information may, in the future, prove to be of some unanticipated value. Also, personal information that has served its purpose and is no longer reasonably expected to support any current or planned activities should not be kept.

10. The ability to acquire certain kinds of personal information does not mean that it is proper to do so. In certain cases, individuals have no choice whether to disclose personal information. For example, if the individual executes a transaction on the NII, personal information in the form of transactional data will typically be generated. In other cases, the choice may exist in theory only. Exercising certain choices may result in the denial of a benefit that individuals need to participate fully in society--for example, obtaining a license to drive an automobile. In such cases, society should establish some basic level of privacy protection in accordance with the Information Privacy Principle (I.A.).

II.B. Notice Principle

Information users who collect personal information directly from the individual should provide adequate, relevant information about:

1. Why they are collecting the information;

2. What the information is expected to be used for;

3. What steps will be taken to protect its confidentiality, integrity, and quality;

4. The consequences of providing or withholding information; and

5. Any rights of redress.

11. Personal information can be acquired in one of two ways: it can be collected directly from the individual or obtained from some secondary source. By necessity, the principles governing these two methods of acquiring personal information differ. While notice obligations can be placed on all those who collect information directly from the individual, they cannot be imposed uniformly on entities that have no such direct relationship. If all recipients of personal information were required to notify every individual about whom they receive data, the exchange of personal information would become prohibitively burdensome, and many of the benefits of the NII would be lost.

12. For those who collect personal information directly from the individual, the Notice Principle requires the individual to be given sufficient information to make an informed decision about his or her privacy. The importance of providing this notice cannot be overstated because the terms of the notice substantially determine the individual's understanding of how personal information will be used, an understanding that must be respected by all subsequent users of that information.

13. The Notice Principle specifically applies to personal information designated by law as a public record and to transactional data generated as a byproduct of a transaction. With respect to transactional data, this principle applies to all parties, including not only the party principally transacting with the individual in order to provide some product or service, but also to those transaction facilitators such as communication providers and electronic payment providers who help to consummate these transactions. For example, if an individual purchases flowers with a credit card through an on-line shopping mall accessed via modem, the Notice Principle applies to all parties who collect transactional data related to the purchase, not only to the florist, but also to the telephone and credit card companies. Transaction

facilitators would ordinarily provide notice at the time they establish an account, or when billing the customer.

14. What counts as adequate, relevant information to satisfy the Notice Principle depends on the circumstances surrounding the collection of information. In some cases--especially where there is a continuing relationship between the individual and the information collector-- notice need not be given before each instance that personal information is collected. For example, an information or communication service provider should ordinarily give notice when the individual subscribes to a particular service and perhaps periodically thereafter, not each time the individual uses the service. In other cases, the ordinary and acknowledged use of personal information is so clearly contemplated by the individual that providing formal notice is not necessary. For example, if an individual's name and address is collected by a pharmaceutical company that takes the order over interactive television simply to deliver the right medicine to the right person at the right address, no elaborate notice need precede taking the individual's order. However, should the pharmaceutical company use the information in a manner not clearly contemplated by the individual--for example, to create and sell a list of people afflicted with high blood pressure to health insurance companies--then some form of notice should be provided.

15. While the Notice Principle indicates what might constitute the elements of adequate notice, it does not prescribe a particular form for that notice. Rather, the goal of the Principle is to ensure that the individual has sufficient information in an understandable form to make an informed decision. Thus the drafters of notices should be creative about informing in ways that will help all individuals, regardless of age, literacy, and education to achieve this goal.

16. Finally, although the Notice Principle requires information collectors to inform individuals what steps will be taken to protect personal information, they are not required to provide overly technical descriptions of such security measures. Indeed, such descriptions might be unwelcome or unhelpful to the individual. Furthermore, they may be counterproductive since widespread disclosure of the technical security measures might expose system vulnerabilities, in conflict with the Protection Principle (II.C.).

II.C. Protection Principle

Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.

17. On the NII, personal information is maintained in a networked environment, an environment that poses tremendous risk of unauthorized access, disclosure, alteration, and destruction. Both insiders and outsiders may gain access to information they have no right to see or may make hard-to-detect changes in data that will then be relied upon in making critical decisions.

18. For example, our health care providers expect to become intensive participants in the NII. Through the NII, a hospital in a remote locale will be able to send x-rays for review by a radiologist at a teaching hospital in another part of the country. The potential benefits are obvious. Yet, such benefits will not be realized if individuals refuse to send such sensitive data because they fear that the NII cannot ensure that sensitive medical data will remain confidential and unaltered.

19. In deciding what controls are appropriate, information users should recognize that personal information should be protected in accordance with the individual's understanding and in a manner commensurate with the harm that might occur if it were improperly disclosed or altered.

20. In protecting personal information, information users should adopt a multi-faceted approach that includes both technical and managerial controls. As for technical controls, information users should, for example, consider encrypting personal information, including the contents of communications and information generated from transactions. In addition, they should consider computerized audit trails, which help detect improper access by both insiders and outsiders. As for management controls, one could strive, for example, to create an organizational culture in which individuals learn about fair information practices and adopt these practices as the norm. Also, organizations could establish policies to forbid information acquired for one activity from being used for another unrelated activity.

II.D. Fairness Principle

Information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.

21. An individual's understanding encompasses the individual's objectively reasonable contemplation and scope of consent when the information was collected. As explained earlier, an individual's understanding depends principally on the notice provided by the information collector pursuant to the Notice Principle (II.B.) and obtained by the individual pursuant to the Awareness Principle (III.A.). Without a Fairness Principle, information use may know no boundaries and thus go beyond the individual's understanding.

22. If an information user seeks to use personal information in an incompatible manner, the user must first notify the individual and obtain his or her explicit or implicit consent. The nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing. In other cases, a notice offering the individual the ability to opt out of the use within a certain specified time may be adequate. Inherent in this principle is the requirement that whenever personal information is transferred from information user to user, the individual's understanding of how that personal information will be used must also be conveyed. Because all information users must abide by the Fairness principle, both information transferor and transferee bear a responsibility to ensure that the individual's understanding is transferred along with the information.

23. In deciding whether a particular use of information is "incompatible" with an individual's understanding, information users should evaluate whether the uses are permitted explicitly in the notice or are otherwise consistent with the notice. Any use of information beyond these conditions is incompatible with the individual's understanding. What is incompatible under this Principle is not limited to what has been interpreted as incompatible under the Privacy Act. *See* 5 U.S.C. § 552a.

24. The Fairness Principle cannot be applied uniformly in every setting. An incompatible use is not necessarily a harmful use; in fact, it may be extremely beneficial to the individual and society. There are some incompatible uses that will produce enormous benefits and have at most a trivial effect on the individual's information privacy interest. Research and statistical studies, in which information will not be used to affect the individual, are examples. Obtaining the consent of the individual to permit new statistical uses of existing data adds cost and administrative complexity to the process and risks impairing the research project. In other cases, personal information may be used for a significant public need recognized by society in a highly formal, open way (typically in legislation) that would be thwarted by giving the individual a chance to limit its use. One example would be the use of personal information in a law enforcement investigation for which the suspect's consent would be unlikely and even asking for such consent would be counterproductive to the investigation. Another example would be an incompatible use of personal information, made by the investigatory press, that is specifically protected and sanctioned by the First Amendment.

II.E. Education Principle

Information users should educate themselves and the public about how information privacy can be maintained.

25. The Education Principle represents a significant addition to the traditional principles of fair information practice. There are many uses of the NII for which individuals cannot rely completely on governmental or other organizational controls to protect their privacy. Although individuals often rely on such legal and institutional controls to protect their privacy, many people will engage in activities outside of these controls, especially as they engage in the informal exchange of information on the NII. Thus, individuals must be aware of the hazards of providing personal information, and must make judgments about whether providing personal information is to their benefit.

26. The full effect of the NII on the use of personal information is not readily apparent, and individuals may not recognize how their lives may be affected by networked information. Because it is important that individuals and information users appreciate how the NII affects information privacy, all information users should participate in education about the handling and use of personal information. Traditionally, governments and schools have educated the public on matters of social rights and responsibilities, and they must continue to play a lead role. However, as major builders of the NII, the private sector has as crucial a role to play. Such education, which would help individuals minimize the risks to their privacy, could involve privacy telephone hotlines, Internet privacy "help" sites, and comprehensive marketing and publicity campaigns.

III. Principles for Individuals Who Provide Personal Information

III.A. Awareness Principle

Individuals should obtain adequate, relevant information about:

1. Why the information is being collected;

2. What the information is expected to be used for;

3. What steps will be taken to protect its confidentiality, integrity, and quality;

4. The consequences of providing or withholding information; and

5. Any rights of redress.

27. Increasingly, individuals are being asked to surrender personal information about themselves. Sometimes the inquiry is straight-forward; for example, a bank will ask for personal information prior to processing a loan request. In this case, one use for the information is clear--to process the loan application. There may, however, be other uses that are not so obvious, such as using some of that information for a credit card solicitation. Indeed, individuals regularly disclose personal information without being fully aware of the many ways in which that information may ultimately be used. For example, an individual may not realize that paying for medical services with a credit card creates transactional data that could reveal the individual's state of health.

28. The Awareness Principle recognizes that although information collectors have a responsibility to inform individuals why they want personal information, individuals also have a responsibility to understand the consequences of providing personal information to others. This is especially true in an interactive realm such as the NII, in which individuals can actively shape the terms of their participation. For example, when individuals have real choices about whether and to what degree personal information should be disclosed, they should take an active role in deciding whether to disclose personal information in the first place, and under what terms.

29. Of course, if individuals are to be held responsible for making these choices, they must be given enough information to make intelligent choices. This is how the Awareness Principle works in conjunction with the Notice Principle (II.B.) and more broadly with the Education Principle (II.E) to enable individuals to take responsibility over how personal information is disclosed and used.

III.B. Empowerment Principles

Individuals should be able to safeguard their own privacy by having:

1. A means to obtain their personal information;

2. A means to correct their personal information that lacks sufficient quality to ensure fairness in its use;

3. The opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions; and

4. The opportunity to remain anonymous when appropriate.

30. Individuals should have a means to obtain from information users a copy of their personal information and to correct information about them that lacks sufficient quality to ensure fairness in its use. The extent to which such means are provided depends on various factors, including the seriousness of the consequences to the individual of using the personal information and any First Amendment rights held by the information user.

31. Further, if the terms of the information collection are unsatisfactory, the individual should consider various self-initiated measures to safeguard privacy. For example, to safeguard the confidentiality or integrity of a communication, the individual should have the opportunity to use appropriate tools such as encryption. Also, to avoid leaving a data trail of transactional records, individuals should have the opportunity to remain anonymous, when appropriate. For example, anonymity would be appropriate when an individual browses a public electronic library or when an individual engages in anonymous political speech protected by the Constitution. *See McIntyre v. Ohio Elections Commission*, 131 L. Ed. 2d 426 (1995). In an ideal world, offering undecipherable encryption or absolute anonymity would serve to protect privacy with no negative effect. Unfortunately, in the real world, some will abuse these technologies and, in the process, harm others. It is beyond the scope of the Principles how encryption or anonymity can be offered to individuals for legitimate uses while minimizing their misuse. These issues must, however, be addressed if the NII is to achieve its full potential.

III.C. Redress Principle

Individuals should, as appropriate, have a means of redress if harmed by an improper disclosure or use of personal information.

32. Redress is required only when an individual is harmed. Designed for general applicability, the Redress Principle does not answer in any particular case whether harm has occurred at all or whether enough harm has occurred to warrant a specific form of redress. Those questions must be answered in the sectoral implementation of the Principles.

33. An improper use specifically includes a decision based on personal information of inadequate quality--information that is not accurate, timely, complete, or relevant for the purpose for which it is provided and used. The Redress Principle does not, however, set the level of culpability on the part of the information user necessary to warrant a specific form of redress.

34. When redress is appropriate, the Principles envision various forms including, but not limited to, informal complaint resolution, mediation, arbitration, civil litigation, regulatory enforcement, and criminal prosecution, in various private, local, state, and federal forums with the goal of providing relief in the most cost-effective manner possible.

PWG/IPC: june6.nii

/1/ *See* Organization for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Annex to Recommendations of the Council of 23rd September 1980.* .

Privacy -GV

April 20, 1998

MEMORANDUM FOR NEC/DPC DEPUTIES

FROM: SALLY KATZEN

RE: NEC/DPC DEPUTIES MEETING ON PRIVACY

The next NEC/DPC meeting on privacy will be on **April 24, 1998 11:00AM** in **Room 472, Old Executive Office Building**. To RSVP, please provide your clearance information to Shannon Mason at (202) 456-2800.

The meeting will have the following agenda:

1. **Agency views on legislative and administrative solutions for specific sectors or types of data.**

We did not have an opportunity at the last meeting to discuss the legal and regulatory options outlined in the April 7th Department of Commerce memo by Becky Burr. This memo discusses not only legislative proposals, but also steps the Administration could take to strengthen the protection of public data about individuals. Agencies should fax or e-mail their views or comments on the options discussed in the memo by COB Wednesday, April 22nd to Tom Kalil (fax: 456-2223, e-mail: kalil_t@a1.eop.gov).

Agencies that are not familiar with the Administration's existing privacy principles can find them on the World Wide Web at:

http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html.

2. **Discussion of privacy entity**

By Tuesday, we will circulate an OMB analysis of the agency comments on the "privacy entity" paper.

3. **Discussion of proposal for self-regulation**

By Tuesday, we will circulate a Commerce analysis of the IBM-led proposal for self-regulation.

202-395-5167, or by electronic mail to BERNSTEIN_M@A1.EOP.GOV. Comments submitted by facsimile or electronic mail need not also be submitted by regular mail.

FOR FURTHER INFORMATION CONTACT: Ms. Maya A. Bernstein, Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Voice telephone: 202-395-4816. Facsimile: 202-395-5167. Electronic mail: BERNSTEIN_M@A1.EOP.GOV

SUPPLEMENTARY INFORMATION: In the Report of the National Performance Review, "Creating a Government that Works Better & Costs Less: Reengineering Through Information Technology," the Vice President tasked the Information Infrastructure Task Force with considering privacy policy with respect to the National Information Infrastructure (NII). The Privacy Working Group first developed "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information" (the Privacy Principles), which described a set of fair information practices appropriate to the NII and which were finalized in June 1995. The next step for the Privacy Working Group was to consider how best to promote those principles. To that end, the Working Group undertook significant research on the state of privacy with respect to the NII, current U.S. law, and private sector practices. That work served as the basis for the Information Policy Committee□,s Option Paper. The Committee is now making the Paper available for comment.

As Vice President Gore predicted in 1995, development of the Global Information Infrastructure (GII) is increasing economic growth and productivity, creating high-wage jobs in newly emerging industries, and fostering U.S. technological leadership across the globe. Through this medium, we can already secure high quality services at low cost and prepare our children for the demands of the 21st Century. A more open and participatory democracy is emerging at all levels of government.

The information economy of the 21st century will run on data. Some of that data may be highly personal and sensitive. In some cases, personal data may become quite valuable. Thus, the transition to the Information Age calls for a reexamination of the proper balance between the competing values of personal privacy and the free flow of information in a democratic society. Will our traditional balance point serve in the digital age? Can we continue to rely on the same tools we have used to strike this balance in the past? Or, is an entirely new approach warranted?

The Options Paper explores the growing public concern about personal information privacy. The paper describes the status of electronic data protection and fair information practices in the United States today, beginning with a discussion of the "Principles for Providing and Using Personal Information," issued by the Information Infrastructure Task Force in 1995. It then provides an overview of new information technologies, which

The Consumer Information Organization

http://consumer-info.org

Office of Management and Budget

22978 Federal Register / Vol. 62, No. 81 / Monday, April 28, 1997 / Notices

OFFICE OF MANAGEMENT AND BUDGET

Options for Promoting Privacy on the National Information Infrastructure

AGENCY: Office of Management and Budget.

ACTION: Notice and request for comments.

DATES: Comments should be submitted no later than June 27, 1997.

SUMMARY: OMB announces the availability of "Options for Promoting Privacy on the National Information Infrastructure" (Options Paper) on behalf of the Information Policy Committee of the National Information Infrastructure Task Force (IITF). This Options Paper results from work performed by the Privacy Working Group and refined by the Committee. The Committee is chaired by the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB). This Options Paper builds upon the October 1995 report of the Privacy Working Group, "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (Privacy Principles), which was published in draft form in the Federal Register on January 20, 1995 (60 Fed. Reg. 4362) and was finalized in June 1995. None of the options presented has been adopted as Administration policy; they are set forth in this document in the belief that they are worthy of public discussion.

DATES: Comments should be submitted no later than June 27, 1997.

ELECTRONIC AVAILABILITY AND ADDRESSES: The options paper is available electronically from the IITF site on the World Wide Web: http://www.iitf.nist.gov/ipc/ipc-pub.html and in paper form from the OMB Publications Office, 725 17th Street, NW, Washington, D.C. 20503, telephone: 202/395-7332, facsimile: 202/395-6137. Comments may be sent to the Information Policy Committee c/o the Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236, Washington, D.C. 20503. Comments may also be submitted by facsimile to 202 395 5167 or by electronic mail to BERNSTEIN_M@A1.EOP.GOV. Comments

shows that personal information is currently collected, shared, aggregated, and disseminated at a rate and to a degree unthinkable just a few years ago. Government is no longer the sole possessor of extensive amounts of personal information about U.S. citizens: in recent years the acquisition of personal information by the private sector has increased dramatically. The paper next considers in more detail the laws and policies affecting information privacy in four specific areas: government records, communications, medical records, and the consumer market. This examination reveals that information privacy policy in the United States consists of various laws, regulations and practices, woven together to produce privacy protection that varies from sector to sector. Sometimes the results make sense, and sometimes they do not. The degree of protection accorded to personal information may depend on the data delivery mechanism rather than on the type of information at issue. Moreover, information privacy protection efforts in the United States are generally reactive rather than proactive: both the public and the private sector adopt policies in response to celebrated incidents of nonconsensual disclosure involving readily discernable harm. Sometimes this approach leaves holes in the fabric of privacy protection.

The paper then turns to the core question: in the context of the Global Information Infrastructure (GII), what is the best mechanism to implement fair information practices that balance the needs of government, commerce, and individuals, keeping in mind both our interest in the free flow of information and in the protection of information privacy? At one end of the spectrum there is support for an entirely market-based response. At the other end of the spectrum, the federal government is encouraged to regulate fair information practices across all sectors of the economy. In between these poles lie a myriad of options.

In response to public concern, both government and private industry seem to be taking a harder look at privacy issues. As government and consumers become more aware of the GII's data collection, analysis and distribution capabilities, demand could foster a robust, competitive market for privacy protection. This raises the intriguing possibility that privacy could emerge as a market commodity in the Information Age. The paper recognizes ongoing efforts to enhance industry self regulation to carry out the IITF Privacy Principles, and also discuss ways this self regulation might be enforced. The paper also discusses a number of ways that government could facilitate development of a privacy market.

The paper then considers a number of options that involve creation of a federal privacy entity. It discusses some of the many forms that such an entity could take and considers the advantages and disadvantages of the various choices. It also considers the functions that such an entity might perform, as well as various options for locating a privacy entity within the federal government.

This paper presents a host of options for government and private sector action. The ultimate goal is to identify the means to maintain an optimal balance between personal privacy and freedom of information values in the digital environment. The next step is to receive and respond to public comment on the report in order to develop consensus regarding the appropriate allocation of public and private sector responsibility for implementation of fair information practices.

Sally Katzen

Administrator, Office of Information and

Regulatory Affairs

[FR Doc. 97-10894 Filed 4-25-97; 8:45 am]

Billing Code 3110-01-P

Download the WordPerfect 5.1/5.2 Version of this Document.

Options for Promoting Privacy

on the

National Information Infrastructure

Draft for Public Comment

Information Policy Committee

National Information Infrastructure Task Force

April 1997

EXECUTIVE SUMMARY

The information revolution is underway.

As Vice President Gore predicted in 1995, development of the Global Information Infrastructure (GII) is increasing economic growth and productivity, creating high-wage jobs in newly emerging industries, and fostering U.S. technological leadership across the globe. Through this medium, we can already secure high quality services at low cost and prepare our children for the demands of the 21st Century. A more open and participatory democracy is emerging at all levels of government.

And yet, we are only beginning to tap the information infrastructure's potential to improve the lives of ordinary Americans.

The information economy of the 21st Century will run on data. Some of that data may be highly personal and sensitive. In some cases, personal data may become quite valuable. Thus, the transition to the Information Age calls for a reexamination of the proper balance between the competing values of personal privacy and the free flow of information in a democratic society. Will our traditional balance point serve in the digital age? Can we continue to rely on the same tools we have used to strike this balance in the past? Or, is an entirely new approach warranted?

This Options Paper explores the growing public concern about personal information privacy. The paper describes the status of electronic data protection and fair information practices in the United States today, beginning with a discussion of the Principles for providing and using personal information issued by the Information Infrastructure Task Force in 1995. It then provides an overview of new information technologies, which shows that personal information is currently collected, shared, aggregated, and disseminated at a rate and to a degree unthinkable just a few years ago. Government is no longer the sole possessor of extensive amounts of personal information about U.S. citizens; in recent years the acquisition of personal information by the private sector has increased dramatically.

We next consider in more detail the laws and policies affecting information privacy in four specific areas: government records, communications, medical records, and the consumer market. This examination reveals

that information privacy policy in the United States consists of various laws, regulations and practices, woven together to produce privacy protection that varies from sector to sector. Sometimes the results make sense, and sometimes they do not. The degree of protection accorded to personal information may depend on the data delivery mechanism rather than on the type of information at issue. Moreover, information privacy protection efforts in the United States are generally reactive rather than proactive: both the public and the private sector adopt policies in response to celebrated incidents of nonconsensual disclosure involving readily discernable harm. Sometimes this approach leaves holes in the fabric of privacy protection.

We then turn to the core question: in the context of the GII, what is the best mechanism to implement fair information practices that balance the needs of government, commerce, and individuals, keeping in mind both our interest in the free flow of information and in the protection of information privacy? At one end of the spectrum there is support for an entirely market-based response. At the other end of the spectrum, we are encouraged to regulate fair information practices across all sectors of the economy. In between these poles lie a myriad of options.

In response to public concern, both government and private industry seem to be taking a harder look at privacy issues. As government and consumers become more aware of the GII's data collection, analysis and distribution capabilities, demand could foster a robust, competitive market for privacy protection. This raises the intriguing possibility that privacy could emerge as a market commodity in the Information Age. We recognize ongoing efforts to enhance industry self regulation to carry out the IITF Privacy Principles. We also discuss ways this self regulation might be enforced, and discuss a number of ways that government could facilitate development of a privacy market.

> create fed privacy entity?

We then consider a number of options that involve creation of a federal privacy entity. We discuss some of the many forms that such an entity could take and consider the advantages and disadvantages of the various choices. We also consider the functions that such an entity might perform, as well as various options for locating a privacy entity within the federal government.

This paper presents a host of options for government and private sector action. Our ultimate goal is to identify the means to maintain an optimal balance between personal privacy and freedom of information in the digital environment. The next step is to receive and respond to public comment on the report in order to develop consensus regarding the appropriate allocation of public and private sector responsibility for implementation of fair information practices.

I.

PRINCIPLES APPLICABLE TO THE COLLECTION AND REUSE OF PERSONAL DATA

1. Background

Fact Sheet # 5: Telemarketing Calls

Privacy Rights Clearinghouse
5384 Linda Vista Rd. #306
San Diego, CA 92110
Voice: (619) 298-3396
Fax: (619) 298-5681
E-mail: prc@privacyrights.org
http://www.privacyrights.org

Telemarketing: Whatever Happened To A Quiet Evening At Home?

Most people have experienced it--that annoying ring of the phone just as dinner goes on the table. When you answer, you find it's not a call from a friend or family member, or even from work. It's someone calling to sell you something--a telemarketer.

How do telemarketers get my telephone number?

There are several ways telemarketers get your number:

1. If you are listed in the **phone book**, they simply may have looked in the White Pages.

2. Several companies compile **national phone directories**, available in CD-ROM and computer databases. These are gathered from local phone books all over the country.

3. The phone company and other businesses publish directories which list people by street address or phone number rather than name. Telemarketers frequently use these **"street address directories"** when they want to call specific neighborhoods. If you are listed in the phone book, you are almost certainly in street address directories, also referred to as "reverse directories."

4. Another way telemarketers obtain your phone number is when **you inadvertently give it to them**. If you sign up for a contest or drawing, a phone number is usually requested. Such give-away promotions may have less to do with gifts than they do with obtaining your number for sales pitches. If you have your phone number printed on your checks, your name, address and phone number can easily be copied and entered into computerized mailing/phone lists.

entered into computerized mailing/phone lists.

5. **Automatic dialing devices** are able to determine all possible phone number combinations, even unlisted numbers, and dial them much more rapidly than any person can.

6. **"800" and "900" numbers** are another way for telemarketers to obtain your phone number. When you call these numbers, your phone number may be captured with a system called "Automatic Number Identification" or ANI. ANI uses equipment which automatically identifies and stores the number from which you are dialing. By matching your phone number with other computerized lists and street address directories, your name and address can often be discovered and added to marketers' databases. Not only will the company that captured your number be able to use it, they may sell it to other marketers.

How can I stop sales calls?

It is difficult to completely eliminate sales phone calls. However, you can dramatically decrease the number of calls you receive by taking the following steps:

1. Sign up for the Direct Marketing Association **Telephone Preference Service** (TPS) to have your phone number added to the DMA's "don't call" list. The major nationwide telemarketers participate in this service. Send your name, address and phonenumber, including your area code, to: **Telephone Preference Service, Direct Marketing Assoc., P.O. Box 9014, Farmingdale, NY 11735-9014**. The TPS will help reduce sales calls but will not eliminate them entirely. Participation by telemarketers is **voluntary**. In addition, the TPS does not stop calls made by automatic or random dialers.

2. When you are contacted by telemarketers, tell them to put you on their **"don't call" list**. Federal laws requires them to maintain and honor such lists. (47 CFR 64.1200; 16 CFR 310)

3. Screen your calls with an **answering machine**.

4. Get an **unlisted phone number**. There are advantages to being listed in the phone book. But if you are tired of being called by telemarketers, having an unlisted number can decrease the volume of calls considerably. Phone companies usually charge a monthly fee for unlisted numbers. To request an unlisted number, call your phone company's business office.

5. Your local phone company may offer some **"custom calling services"** like Caller ID and Call Block which can be used to limit unsolicited calls. Some private companies also sell special equipment that blocks unwanted calls. (See PRC fact sheet 3 on "harassing phone calls" and fact sheet number 19 on

listing be removed

street address

directories

inadvertently release your phone number

"Caller ID.")

6. Call the phone company's business office and request that your from the phone company's street address directory. Also, write or call the major companies that compile and request that your listing be removed:

- ☐ Haines & Company, Inc., Criss-Cross Directory, Attn: Director of Data Processing, 8050 Freedom Ave. N.W., North Canton, OH 44720. (800) 562-8262 (CA only). Calls from outside California (714) 870-8151.
- ☐ R. L. Polk & Co., Attn: List Suppression File, 6400 Monroe Blvd., Taylor, MI 48180-1814. (313) 292-3200. You should give your name, address and ZIP code.

7. Be aware of ways that you . Don't have your phone

number printed on your checks. Consider providing your work number when you **must** give a number. Be sure the requestor has a reasonable need to obtain your number.

8. When calling an **"800" or "900"** number, tell the representative that you do not want your name, address and phone number rented or sold to others. Also request that they do not call you in the future.

Are there any laws about telemarketing?

Yes, both federal and state laws regulate telephone solicitations.

Federal laws

There are two major federal laws that regulate telemarketing. They somewhat overlap. The Telephone Consumer Protection Act of 1991 (TCPA) focuses on the use of telephone lines, and is regulated by The Federal Communications Commission (FCC). (47 USC 227; 47 CFR 64.1200) The Telemarketing and Consumer Fraud Abuse Prevention Act deals with scams and is regulated by The Federal Trade Commission (FTC). (15 USC 6101-6108; 16 CFR 310)

Telephone Consumer Protection Act of 1991 (TCPA)

1. **"Do not call" lists**. The TCPA requires telemarketers to take you off their list if you ask them to do so. Further, telemarketers must have a written policy for maintaining do not call lists, available upon demand. (47 CFR 64.1200) If you have received more than one call by or on behalf of the same company in one year, after you have told the company to place your name on the "do not call list," you can:

- ☐ Sue the telemarketer in state court (usually small claims is recommended) to stop such calls and/or to recover a penalty. The penalty is actual monetary loss or *up to* $500, whichever is greater, for *each* call received after you requested to be placed on the "do not call" list. If the court finds that the marketer willfully or knowingly broke the law, the penalty is up to three times the actual monetary loss or *up to* $1500, whichever is greater.

  The penalty for violations with respect to automatic dialing systems, prerecorded messages and facsimile machines, is *$500* or actual damages, whichever is greater. The penalty for willful or knowing violations is *$1500* or three times the actual damages.
- ☐ File a complaint with the Federal Communications Commission (FCC) and request that it take enforcement action against the telemarketer.
- ☐ Request that the Attorney General in your state file a suit against the telemarketer. If the Attorney General receives several complaints against the same telemarketer, it may take action against the telemarketer.

Calls by or on behalf of tax-exempt nonprofit organizations are *not* required to comply with the "do not

Privacy tip:

keep a log

Restricted hours

Calls by or on behalf of tax exempt nonprofit organizations are required to comply with the "do not call" list requirements. (47 CFR 64.1200) The "do not call" list requirements also do not apply to marketers calling businesses.

If you want to take action against a company that continues to call, send a certified letter, return receipt requested, demanding to be placed on the "do not call" list. Keep a copy of the letter and the return receipt as proof. Also, of all calls.

2. . Telemarketers can only make calls to residences between 8 a.m. and 9 p.m. unless

they have your prior express consent or if you have an established business relationship. (64 CFR 64.1200)

3. **Fax machines**. A telemarketer cannot use a fax machine, computer or other device to send an unsolicited ad to a fax machine unless the receiving party has given prior express consent. Any message sent by fax must clearly mark the following in the margins at the top or bottom of each transmitted page of the message or the first page of each transmission: the date and time it is sent; the sender; and, the phone number (not a 900 number) of the sender or of the sending machine. Fax machines manufactured on or after December 20, 1992, must clearly mark this information on the first page or on each page of the transmission. (47 USC 227) Fax modem boards manufactured on or after December 13, 1995, must also follow these requirements. (47 CFR 68.318)

4. **Recorded messages and automatic dialing devices.** Under the TCPA, a telemarketer cannot place a call to a residence using a prerecorded message unless the called party consents or the call is for emergency purposes. Calls with prerecorded messages are allowed when they are for noncommercial purposes; from someone with whom you have a prior business relationship; from a tax-exempt nonprofit organization; or when they do not include an unsolicited ad.

Autodialed and/or prerecorded messages to emergency numbers, hospitals, cellular telephones, pagers, or any service for which the called party is charged for the call are prohibited. However, they are allowed in emergencies or if the person called has given their prior express consent.

Finally, prerecorded messages are required to state the identity of the business, individual or other entity making the call at the beginning of the message. The telemarketer must provide its address or telephone number (other than a 900 number or the number of the autodialer or prerecorded message player). Any prerecorded call made using an autodialer must release your line within five seconds after you have hung up. (47 USC 227)

The Telemarketing and Consumer Fraud Abuse Prevention Act

1. **"Do not call" lists.** The Telemarketing and Consumer Fraud Abuse Prevention Act also makes it illegal for a telemarketer to call you after you have requested not to be called. And it requires telemarketers to keep "do not call" lists. (16 CFR 310.4) You can sue telemarketers who violate thislaw.

Restricted hours.

isclosures.

However, it is more difficult to sue under this law than under the TCPA. You can only sue in federal court and must show damages greater than S50,000. If you cannot sue the telemarketer, contact the Attorney General's office or FTC. They are also given the right to sue telemarketers for violations of this law.

"Do not call" requirements do not apply to nonprofit organizations. But they do apply to for-profit telemarketing companies providing services for nonprofit organizations if those telemarketers sell goods and services as part of the call.

2. Telemarketers may only call residences between the hours of 8 a.m. and 9 p.m. unless they have the prior express consent of the person called.

3. **D** Telemarketers must promptly make certain disclosures including, that it is a sales call; what they are selling; and the identity of the seller. If the call is for a prize promotion, they must tell you that no purchase or payment is required to win a prize or participate in a prize promotion. (16 CFR 310.4) Before the customer pays, the telemarketer must disclose the total costs of the goods, any

restriction on getting or using them and whether all sales are final or non-refundable. If the call is for a prize promotion, they must tell you the odds for winning, that no purchase or payment is required to win and all material costs or conditions to receive the prize. (16 CFR 310.3)

4. **No misrepresentation.** Telemarketers cannot misrepresent any information including the total cost and the quality of any goods or services. In addition, telemarketers may not make false or misleading statements to persuade you to purchase any goods or services. (16 CFR 310.3)

5. **Checking accounts.** Telemarketers cannot obtain or withdraw money from your checking, savings or similar accounts without your express verifiable authorization. (16 CFR 310.3)

California Laws

1. **Registration.** Certain categories of telemarketers doing business in California must register with the Attorney General's office. The categories of telemarketers covered by this law include companies offering prizes; investments, including metals and coins; office supplies; and items below normal costs. (California Business & Professions Code 17511)

2. **Disclosure.** The telemarketer must disclose specific information at the time he/she is making the sales pitch. The disclosures depend on the type of goods or services the telemarketer is selling. For example, a telemarketer selling office equipment or supplies below normal costs must disclose the address of the location he/she is calling from and the name of the manufacturer of each of the items being sold. (See California Business & Profession Code 17511.5 for a list of disclosures.)

3. **Recorded messages.** Unsolicited prerecorded calls for the sale or lease of goods or services are banned unless a "live" operator first asks permission to play the tape. The operator must also tell the person who answers the phone the name of the caller and either the caller's address or telephone number. The operator must also ask if the person consents to hear the recorded message. Companies can use recorded messages when they contact established customers or if you have requested their call. (California Civil Code 1770 (v))

If you have suffered damages as a result of prerecorded calls, you may sue to recover damages, stop the calls, restore your property and/or obtain other relief that the court believes you deserve. (California Civil Code 1780)

4. **Automatic dialing-announcing devices.** Calls placed using automatic dialing-announcing devices are

Calls placed using automatic dialing-announcing devices are prohibited unless a "live" operator first makes an announcement to the person called. The operator must state the nature of the call and the name, address and telephone number of the business. The caller must also inquire if the person consents to hear the prerecorded message. This requirement does not apply to law enforcement or other specified agencies that use the automatic dialing-announcing device to provide information relating to public safety, police or fire emergencies. (California Public Utilities Code 2872-2874)

Automatic dialing-announcing devices may be used if the person being called has given prior consent; there is a prior business relationship; they have requested the call; or, for other specified purposes including a school contacting a student's parent/guardian regarding attendance. (California Public Utilities Code 2872, 2873) Further, automatic dialing-announcing devices may only be used in California to place calls received in California after 9:00 a.m. and before 9:00 p.m. (California Public Utilities Code 2872)

The California Public Utilities Commission (CPUC) imposes penalties for violations of the use of automatic dialing-announcing devices. The penalty is a fine up to $500 for each violation and/or disconnection of the telephone service to the automatic dialing-announcing device for a period of time as specified by the CPUC. (California Public Utilities Code 2876)

Other laws

Automatic Number Identification. Federal law places restrictions on the use and sale of your phone number when you call an 800 or 900 number. When you call these numbers, your phone number could be captured by Automatic Number Identification (ANI.) According to regulations issued by the Federal Communications Commission, a caller's consent is required before a company can reuse or sell ANI information. However, a company may reuse ANI information to market a product or service that is directly related to the product or service the caller previously purchased. (47 CFR 64.1602) California phone companies which offer ANI must notify their customers that the use of an 800 or 900 number may result in the disclosure of the caller's telephone number to the called party. (California Public Utilities Code 2891.2)

How can I discourage telemarketers?

Tell the telemarketer to put you on their "do not call" list. **Be sure to keep a log** of every time you ask to be put on a company's "do not call" list. Ask for a copy of their written policy for maintaining "do not call" lists. We have also found it effective to say, "I never buy anything over the phone. Please take me off your list." By emphasizing that as a matter of principle you **never** make a purchase when contacted by phone, many telemarketers will remove you from their list.

For more information

To obtain information on whether a specific **telemarketing** company is registered in California, write or call: **California Office of the Attorney General**, Consumer Law Section, 300 S. Spring Street, 5th Floor, Los Angeles, CA 90013. (213) 897-2631.

Complaints may be made to:

- **California Office of the Attorney General**, Public Inquiry Unit, P.O. Box 944255, Sacramento, CA 94244-2550. Telephone: (800) 952- 5225 California only. Calls from outside of California (916) 322-3360.
- **Federal Communications Commission**, Informal Complaints and Public Inquiries Branch, Enforcement Division, Common Carrier Bureau, Mail Stop 1600A2, Washington, D.C. 20554
- **Federal Trade Commission**

utomatic umber denti ication

Cali ornia ice o the ttorney eneral

ederal Communications Commission

- ☐ **F I _**, Public Reference Branch, Room 130, 6th Street and Pennsylvania Ave. NW, Washington, D.C. 20580, Telephone: (202) 326-3128. You can also call your local FTC office.

Complaints about **A N I f** may be made to:

- ☐ **f Off f A G** , Public Inquiry Unit, P.O. Box 944255, Sacramento, CA 94244-2550. Telephone: (800) 952- 5225 California only. Calls from outside of California (916) 322-3360.
- ☐ **F** , 2025 M Street NW, Washington, D.C. 20544.

For a "stop the calls" telemarketing kit, send $3.00 to: **Center for the Study of Commercialism**, 1875 Connecticut Ave. NW, #300, Washington D.C. 20009. Telephone : (202) 332-9110 x393. The kit contains information, tips and forms to keep track of "do not call" requests. It also provides advice on taking your complaint to small claims court.

For a $20 annual fee, **Private Citizen**, a nonprofit organization, will list you in its "do not call" Private Citizen Directory which is distributed twice a year to over 1,400 telemarketing firms. Call (800) CUT-JUNK.

To report fraud and/or to request information on fraud, contact the National Fraud Information Center at (800) 876-7060.

NOTE: The Privacy Rights Clearinghouse does not rent, sell or trade its mailing list with any other organization or company. Your name, address and phone number are kept completely confidential.

HOME

A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE
EXECUTIVE SUMMARY

The Internet has the potential to become the United States' most active trade vehicle within a decade, creating millions of high paying jobs. In addition, Internet shopping may revolutionize retailing by allowing consumers to sit in their homes and buy a wide variety of products and services from all over the world.

See H.R. 1054. policy vs. State + local interference w/ interstate commerce on Internet

Many businesses and consumers are wary of conducting extensive business electronically, however, because the Internet lacks a predictable legal environment governing transactions and because they are concerned that governments will impose regulations and taxes that will stifle Internet commerce.

A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE outlines the Administration's strategy for fostering increased business and consumer confidence in the use of electronic networks for commerce. The paper reflects widespread consultation with industry, consumers groups, and the Internet community.

The paper presents five principles to guide government support for the evolution of electronic commerce and makes recommendations about nine key areas where international efforts are needed to preserve the Internet as a non-regulatory medium, one in which competition and consumer choice will shape the marketplace. With respect to these areas, the paper designates lead U.S. government agencies and recommends international fora for consideration of each issue.

PRINCIPLES

1. The private sector should lead. The Internet should develop as a market driven arena not a regulated industry. Even where collective action is necessary, governments should encourage industry self-regulation and private sector leadership where possible.

2. Governments should avoid undue restrictions on electronic commerce. In general, parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. Governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures or new taxes and tariffs on commercial activities that take place via the Internet.

3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce. Where government intervention is necessary, its role should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, and facilitate dispute resolution, not to regulate.

4. Governments should recognize the unique qualities of the Internet. The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. Accordingly, the regulatory frameworks established over the past 60 years for telecommunication, radio and television may not fit the Internet. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.

5. Electronic commerce on the Internet should be facilitated on a global basis. The Internet is a global marketplace. The legal framework supporting commercial transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller reside.

RECOMMENDATIONS

The principles described above guide the following recommendations:

1. Tariffs and Taxation. The Internet should be declared a tariff-free environment whenever it is used to deliver products and services. The Internet is a truly global medium, and all nations will benefit from barrier-free trade across it.

No new taxes should be imposed on Internet commerce. Existing taxes that are applied to electronic commerce should be consistent across national and subnational jurisdictions and should be simple to understand and administer. State and local governments should cooperate to develop a uniform, simple approach to the taxation of electronic commerce, based on existing principles of taxation.

2. Electronic Payment Systems. The commercial and technological environment for electronic payments is changing rapidly, making it difficult to develop policy that is both timely and appropriate. For these reasons, inflexible and highly prescriptive regulations and rules are inappropriate potentially harmful. In the near-term, case-by-case monitoring of electronic payment experiments is preferable to regulation.

3. Uniform Commercial Code for Electronic Commerce. In general, parties should be able to do business with each other on the Internet under the terms and conditions they agree upon. Private enterprise and free markets have typically flourished, however, where there are predictable and widely accepted legal principles supporting commercial transactions.

The U.S. supports the development of an international uniform commercial code to facilitate electronic commerce. Such a code should encourage governmental recognition of electronic contracts; encourage consistent international rules for acceptance of electronic signatures and other authentication procedures; promote the development of alternative dispute resolution mechanisms for international commercial transactions; set predictable ground rules for exposure to liability; streamline the use of electronic registries.

4. Intellectual Property Protection. Commerce on the Internet will often involve the sale and

licensing of intellectual property. To promote electronic commerce, sellers must know that their intellectual property will not be stolen and buyers must know that they are obtaining authentic products. Clear and effective copyright, patent, and trademark protection is therefore necessary to protect against piracy and fraud.

The recently negotiated World Intellectual Property Organization (WIPO) treaties for copyright protection should be ratified. Issues of liability for infringement, application of the fair use doctrine, and limitation of devices to defeat copyright protection mechanisms should be resolved in a balanced way, consistent with international obligations.

The government will study and seek public comment on the need to protect database elements that do not qualify for copyright protection and, if such protection is needed, how to construct it.

The Administration will promote global efforts to provide adequate and effective protection for patentable subject mater important to the development of the Global Information Infrastructure (GII), and establish standards for determining the validity of patent claims.

The Administration also will work globally to resolve conflicts that arise from different national treatments of trademarks as they relate to the Internet. It may be possible to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage trademark laws on a global basis.

The Administration will review the system of allocating domain names in order to create a more competitive, market based system and will seek to foster bottom-up governance of the Internet in the process.

5. Privacy. It is essential to assure personal privacy in the networked environment if people are to feel comfortable doing business across this new medium.

Data gatherers should tell consumers what information they are collecting and how they ir 1 to use it. Consumers should have meaningful choice with respect to the use and re-use of personal information. Parents should be able to choose whether or not personal information is collected from their children. In addition, redress should be available to consumers who are har by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete or irrelevant personal information.

The Administration supports private sector efforts now underway to implement meaningful, user friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, private sector adoption of and adherence to fair information practices, and dispute resolution. The government will work with industry and privacy advocates to develop appropriate solutions to privacy concerns that may not be fully addressed by industry through self-regulation and technology.

6. Security. The GII must be secure and reliable. If Internet users do not believe that their communications and data are safe from interception and modification, they are unlikely to the

Internet on a routine basis for commerce. The Administration, in partnership with industry, is taking steps to promote the development of a market driven public key infrastructure that will enable trust in encryption and provide the safeguards that users and society will need.

7. Telecommunications Infrastructure and Information Technology. Global electronic commerce depends upon a modern, seamless, global telecommunications network and upon the "information appliances" that connect to it. In too many countries, telecommunications policies are hindering the development of advanced digital networks. The United States will work internationally to remove barriers to competition, customer choice, lower prices, and improved services.

8. Content. The Administration encourages industry self-regulation, the adoption of competitive content rating systems, and the development of effective, user-friendly technology tools (e.g. filtering and blocking technologies) to empower parents, teachers, and others to block content that is inappropriate for children.

The government will seek agreements with our trading partners to eliminate overly burdensome content regulations that create non-tariff trade barriers.

9. Technical Standards. The marketplace, not governments, should determine technical standards and other mechanisms for interoperability on the Internet. Technology is moving rapidly and governments attempts to establish technical standards to govern the Internet would only risk inhibiting technological innovation.

COORDINATION

The Administration will continue to coordinate its approach to electronic commerce. The interagency team that developed this framework and strategy will continue to meet to update the strategy and facilitate its implementation as events unfold.

Background on President's Memorandum for Department and Agency Heads

The President today issued a memorandum for the heads of all Executive Branch Departments and Agencies directing them to implement the strategy outlined in A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE.

The memorandum first instructs Executive Branch officials to apply the Framework's five basic principles to any actions they take with respect to electronic commerce. These principles call for the Internet to function as a market-driven environment with minimal government regulation, and for the Internet to be governed by a consistent set of rules across state, national and international borders.

The memorandum then lists 13 specific objectives and designates appropriate Executive Branch officers to head government efforts to achieve these objectives. In several cases, the memorandum directs Executive Branch officers to achieve specific objectives within the next 12 months.

1. The memorandum directs the US Trade Representative to secure international agreement within the next 12 months to reduce tariffs on Internet related equipment to zero and to ensure that products and services delivered across the Internet are not subject to tariff.

2. The memorandum directs the Secretary of Commerce to seek domestic and international agreement within the next 12 months on common approaches for the authentication of electronic transactions through technologies such as digital signatures.

3. The memorandum directs the Secretary of Commerce and the Director of the Office of Management and Budget to encourage private sector development and deployment within the next twelve months, of effective, industry-developed codes of conduct and technology tools to protect privacy online, especially with respect to children.

4. The memorandum directs the Secretary of Commerce to encourage the development of user-friendly filtering technologies and private rating systems within the next twelve months that empower parents, teachers, and other Internet users to block content that they deem inappropriate for their children.

5. The memorandum directs the Secretary of the Treasury to work with domestic and foreign government officials to assure that no new taxes are imposed on Internet commerce and that existing taxes are applied in ways which do not hinder nor distort commerce.

6. The memorandum directs the Administrator of the General Services Administration to bring federal government purchasing into the electronic age by arranging for federal purchasing of four million items online within the next twelve months.

7. The memorandum directs the Secretary of Commerce to support efforts to establish a private, competitive system for allocating domain names and to create a contractually based self-regulatory regime to resolve conflicts between domain name usage and trademark laws globally.

8. The memorandum directs the Secretary of Treasury to work domestically and internationally to ensure that no new taxes are imposed on Internet commerce, that existing taxes are technology neutral and avoid inconsistent tax jurisdiction and double taxation problems.

9. The memorandum directs the Secretary of Commerce to work globally to support development of a "Uniform Commercial Code" for cyberspace that recognizes, facilitates, and enforces electronic agreements worldwide.

10. The memorandum directs the Secretary of Commerce to support private sector development of technical standards for the Internet and direct the US Trade Rep to oppose governmental efforts to mandate standards or use standards as non-tariff trade barriers.

11. The memorandum directs the Secretary of Treasure to monitor emerging electronic payment technology, to oppose government efforts to regulate electronic payment at this time, and to work with the private sector to ensure that any necessary government activity in this area can flexibly accommodate the needs of the emerging marketplace.

12. The memorandum directs all agencies to work domestically and internationally to make the Internet a secure environment for commerce, supported by a robust infrastructure , and well trained Internet users who understand how to protect their systems and their data.

13. The memorandum directs the Secretary of Commerce to enhance the ability of our patent system to protect patentable innovations in the electronic age, and to work to ensure that patentable subject matter important to global commerce is protected globally.

The memorandum establishes an interagency group under the leadership of the Vice President to coordinate implementation of the government's strategy for electronic commerce and directs agency heads to report to him through the interagency group every six months on progress towards meeting all of the specific objectives outlined in the memorandum.

Internet Pioneers In Attendance:

Tim Berners-Lee - Director, World Wide Web Consortium; Inventor of the World Wide Web; Cambridge, MA.
Vint Cerf - Senior VP, Internet Architecture and Engineering, MCI Communications Corp.; Founding President, Internet Society; co-inventor of the computer-networking protocols that enabled the development of the internet; Reston, VA.
Robert Kahn - President, Corporation for National Research Initiatives; co-inventor of the computer-networking protocols that enabled the development of the internet; Reston, VA.
Esther Dyson - President, EDV Holdings; Member, President's National Information Infrastructure Advisory Council; Chair, Electronic Frontier Foundation; New York, NY.
David Duke - Corning; Head of research team at Corning that developed fiber optics; Corning, NY

Electronic Commerce Business and Internet Leaders available at the stakeout immediately following the event:

Business Leaders:

Louis Gerstner, Chairman & CEO, IBM Corp, Armonk, NY
Macdara MacColl, Managing Director, Parent Soup, New York, NY
Steve Case, CEO, Chairman & President, America Online, Inc., Dulles, VA
Robert Palmer, Chairman & CEO, Digital Equipment Corporation, Maynard, MA
Carl Pascarella, President & CEO, Visa International, San Francisco, CA
Eric Schmidt, CEO, Novell Inc., San Jose, CA
Tara Lemmey, CEO & Co-Founder, Narrowline, New York, NY

Internet Leaders:

Tim Berners-Lee - Director, World Wide Web Consortium; Inventor of the World Wide Web.
Vint Cerf - Senior VP, Internet Architecture and Engineering, MCI Communications Corp.; Founding President, Internet Society; co-inventor of the computer-networking protocols that enabled the development of the internet
Robert Kahn - President, Corporation for National Research Initiatives; co-inventor of the computer-networking protocols that enabled the development of the internet.
Esther Dyson - President, EDVenture Holdings; Member, President's National Information Infrastructure Advisory Council; Chair, Electronic Frontier Foundation
Jerry Berman - Executive Director, Center for Democracy and Technology ,a non-profit foundation working to advance democratic values and constitutional liberties on the internet.