- VP Speech May 14
- July 1st Commerce

~~May~~
July 1st - electronic commerce
→ ~~April event~~ -
Housing
→ June event

DRAFT1 **Memorandum**

To: WH/NEC/OVP

From: DOC (Becky Burr, Andy Pincus)

Re: Proposed Action Plan for Privacy

Date: March 18, 1998

Commerce

Americans are worried about their privacy. A recent series of articles in the Washington Post, as well as a recent Businessweek article reflect growing concern on this issue and highlight the importance of strong leadership in this area.

We believe that public concern is focused on three areas: medical information, financial information, and "profiling" or "datamining" – the practice of creating detailed electronic dossiers by bringing together an array of facts from scattered database sources.

The Clinton Administration has been aggressive about privacy protection (*see* "Clinton Administration Privacy Accomplishments," attached). Nonetheless, more can be done to enhance privacy protection.

Medical/Genetic Privacy:

The Administration has called for legislation to protect the privacy of medical records and genetic information. The Administration may want to reinforce this position by supporting specific legislation. In addition, California is now considering legislation to protect biometric information. We should consider supporting similar federal legislation along these lines.

Financial Privacy:

The Administration supported 1996 amendments to the Fair Credit Reporting Act that strengthen financial privacy by establishing "opt-out" obligations for prescreening for credit opportunities, impose new obligations on creditors with respect to the accuracy of information furnished to consumer reporting agencies, establish new reinvestigation and notice obligations, and impose significant new consent requirements to obtain reports containing medical information and reports for employment purposes.

FTC enforcement pf the FCRA is focused on the "big three" credit reporting agencies. The FCRA initially applied only to credit reporting agencies. The 1996 Amendments extended coverage to the millions of entities (including employers) that furnish information to credit reporting agencies. In addition, a large number of database companies providing financial information on the Internet are in fact covered by the Fair Credit Reporting Act (e.g. the Medical Information Business, Acxion, etc.). The Administration could reinforce its support for financial privacy by calling for stepped up enforcement of the FCRA by the Federal Trade Commission.

The FTC has authority, under Section 5 of the FTC Act, to pursue unfair or deceptive practices in commerce, which it will use to enforce adherence with fair information practices. This authority extends to non-depository lending/financial institutions (American Express, Household Finance, etc.). The Treasury/Comptroller of the Treasury has similar authority that applies to depository institutions under Reg AA. Treasury could clarify its willingness to use Reg AA in the privacy area.

Profiling:

The information used to create a data profile has been available for many years. Only in recent years, however, has it become technologically and economically feasible to combine information from the many databases. As a result, marketers and insurers can access detailed information about an individuals personal needs, lifestyle and spending habits.

An enormous amount of this information comes from "public" data sources. The Clinton Administration could address concern about public information on a number of levels.

First, the Administration could issue an executive order or executive memorandum that ensures full compliance with the Privacy Act. OMB could provide guidance for federal agencies on appropriate use of the "routine use" exemption. In addition, States receive information from the federal government (for matching purposes to identify, for example, child support cheats) pursuant to MOUs in which the States promise to maintain confidentiality. The Administration could direct agencies to conduct audits and investigate allegations that some States don't abide by this requirement.

Second, the Administration could investigate State compliance with statutes like the Driver's Privacy Protection Act of 1994, under which States must afford motor vehicle registrants to licensed drivers an opportunity to choose not to make their data available before their personal information is released.

Third, the Administration could undertake a re-evaluation of the appropriate use of "public" information in general. Does the government need all of the information it collects and disclosed, or should the Administration begin an initiative to reduce data collection (and thereby disclosure) and urge the States to follow the same course? Should some types of public information be made available only in paper form (and not in searchable databases)? Can/should the government prohibit the use of government databases (or databases compiled from public records) for "profiling purposes"? (Obviously, open government/First Amendment issues will have to be considered in this context.)

Fourth, the Administration could undertake a study of non-governmental use of social security numbers for identification purposes, looking toward some sort of enhanced prohibition on their use.

Fifth, the Administration could consider proposing legislative or regulatory restrictions on "profiling" businesses (and profiling activities by other types of businesses) analagous to the FCRA that would give consumers some choice with respect to use of personal data for this purpose, or at least to know what is going on)?

Internet:

→ high level enforcement

We should also be able to significantly enhance privacy protection online.

Sectoral specific statutes applicable to personal information (e.g. medical records, FCRA, video rental records, etc.) apply to information on the Internet. But because networked communication technology facilitates datamining and seamlessly creates transactional records, privacy concerns often surface with regard to the Internet. **Administration spokespersons should stress that existing statutory protections and regulatory obligations apply to personally identifiable information on the Internet.**

Keeping in mind that the Internet is often simply a conduit, the nature of the Internet makes regulatory solutions less likely to provide real privacy benefits. On July 1 the Commerce Department and OMB will report to the President on private sector implementation of effective self regulation for privacy, including codes of conduct, industry developed rules, technological solutions to protect privacy on the Internet, and means for ensuring the privacy of children online. **At this point industry leaders have committed to establishing an overarching enforcement mechanism to ensure that self regulatory schemes (1) are easy for consumers to recognize (seals), (2) comport with fair information practices, (3) verify compliance through audits and other procedures, (4) provide prompt and efficient dispute resolution and recourse for consumers harmed by misuse of personal information, and (5) that those who violate privacy policies suffer appropriate consequences (trade association disciplinary measure, revocation of seals, etc.)**

In anticipation of this report, the Department of Commerce has adopted the following action plan on online privacy:

Website: The Department will establish an Internet website (linking from "www.ecommerce.gov") to provide more information about DOC's efforts to promote self regulation and other mechanisms to assure online privacy, as well as to disseminate information about privacy events in April and June. The website would include contact information, electronic postings of requests for comments and information about paper and electronic submissions, schedules of upcoming meetings, and documents and draft working papers.

Request for Comment: DOC will shortly issue a request for public comment on (1) the Elements of Effective Self Regulation for Protection of Privacy (staff draft), (2) self regulation as a mechanism for protecting privacy online, (3) alternatives to self regulation for online privacy, and (4) views, concerns, and experiences regarding Internet privacy.

Elements of Effective Self Regulation: The Department of Commerce has released a discussion paper, Elements of Effective Self Regulation for comment in the business, public interest, advocacy and international community. This paper outlines the enforcement mechanisms that must be in place for self-regulation to work (i.e. systems for compliance verification, dispute resolution, and consequences). This paper will be refined in light of public comment.

Methodology/Criteria for Evaluating Self Regulation: The Department of Commerce has issued a call for papers proposing a methodology and objective criteria for evaluating whether or not a particular self regulation program is effective and succeeds in meeting the goals set out in the elements paper. Paper submitted would also be published in the Federal Register for public comment, and would be the subject of a public "peer review" at the April privacy event. As a result of this public vetting, the methodology/criteria paper would be refined and finalized.

April 23,24

Privacy Event -- April/early May: This two-day DOC event is planned to establish a baseline for evaluating self regulation as a mechanism for protecting privacy online. The conference will serve several purposes. First, it will raise consumer awareness of privacy issues; second, it will allow companies to begin to present the status of their efforts toward self regulation based on the elements paper; third, it will allow a full and fair discussion of the role that self regulation can play in online privacy protection, fourth, it will allow presentation and public discussion of a proposed methodology for evaluating self regulation, and fifth, it will set the stage for further evaluation of privacy protection technology. It is important that public interest groups and privacy advocates participate in this meeting to assure a fair and thorough airing of views as well as the representation of these groups in the process. The results of the meeting will feed into the June meeting. (See proposed agenda, attached.)

Privacy Event – June: The June meeting is planned to continue the **process** of evaluating business efforts toward effective self regulation and the development of consumer empowerment technology for privacy protection. We would examine sectoral privacy policies, as refined by input in April, and industry developed enforcement mechanisms.

Privacy Event – Mid May: If significant progress has been made in the private sector, we would hold an event to highlight private sector initiatives that meet our self regulatory standards.

Privacy Entity:

OMB/DOC reps are working on an memo designed to help answer questions about the appropriate role of the government in the area of privacy protection. There appears to be some consensus that privacy issues could be better coordinated. Assuming consensus arises with respect to coordination functions, the Administration may want to formally announce a system of enhanced coordination at the federal level.

Marya Bensha   # 3131

Where

What

Consumers

privacy conf.

4/8 - Dept

5/1 DOC - conf

5/14 - VP Speech - encryption

7/1 - Electronic Commerce - direction deadline
Magazine paper - self-reg'l mechanism

54815

Agenda for NEC/DPC meeting on privacy
March 19, 1998

1. Process

    - NEC/DPC Deputies meeting on privacy in April

2. Creation of "privacy entity"

3. Specific initiatives

- Medical records
- Genetic privacy
- Consumer bill of rights/financial privacy
- Internet/e-commerce
- Others?

4. Promoting Administration's privacy principles

5. U.S.-EU relationship

Agenda for NEC/DPC meeting on privacy
March 19, 1998

GW

1. Process

   - NEC/DPC Deputies meeting on privacy in April

2. Creation of "privacy entity" OMB DOC, 2/3 - Sally Katzen
   - Agencies
   - what functions
     - coordination
       - Surgeon Gen'l
       - Symbolic

3. Specific initiatives

   - Medical records — SB medical records
   - Genetic privacy — SB preemption
   - Consumer bill of rights/financial privacy — Transiting
     - placement
     - wireless side
   - Internet/e-commerce — IBM Commerce profiling
     10-40 businesses
     seals for compliance
     - BBureau
   - Others? profiling -
     - leg. affairs

4. Promoting Administration's privacy principles
   - 1800 privacy #

5. U.S.-EU relationship Commerce
   - Central
   - Mid May announcement Single phone #
   - Trustee

IBM
Amex
EDS
ATT
Citibank

Credit

Kids -

deceptive practices

Europeans → IBM - assured Daley

Maya Bernstein
OMB x54816

next proposal

Clinton Presidential Records
Digital Records Marker

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

This marker identifies the place of a publication.

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

privacy Privacy -9W

Individual Reference Services

A Report to Congress

Federal Trade Commission

December 1997

P

EW

[illegible]

MEMORANDUM

TO: TOM FREEDMAN, MARY L. SMITH

FROM: DREW HANSEN

RE: FEDERAL GOVERNMENT PRIVACY ISSUES

DATE: AUGUST 12, 1997

Some examples of privacy issues within the federal government:

- **IRS.** Since late 1994, more than 700 IRS employees have been punished for improperly accessing agency information. Richard W. Czubinski, a former KKK member, used his position at the IRS to look up returns of a political opponent, a family adversary, and two associates in the white supremacist movement. His conviction was thrown out because the prosecution did not prove that he used the information or disclosed it to anybody. A GAO report released on April 10, 1997 contended that the IRS system to track "browsing" is cumbersome and cannot produce well-targeted results. Recently addressed by P.L. 105-35 (August 5, 1997).

- **Social Security Administration.** The SSA shut down its Internet site in April after complaints that individual records were not adequately protected. The SSA is considering measures such as digital signatures, passwords, and PIN numbers to secure the site. In 1996, a caseworker in the New York City Human Resources Administration persuaded ten SSA employees to provide him with personal information from the files of 11,000 Americans. The caseworker then used this information in a credit fraud scheme.

- **Federal Prisons.** Federal prisoners are engaged in data entry for the IRS and other public agencies. Inmates in 27 state prison systems handle public records. Convicted rapists and pedophiles often have access to personal information, allowing them to conduct detailed harassment campaigns.

- **Law Enforcement.**

    - In late 1996, the telecommunications industry fought the FBI over an FBI proposal to mandate the installation of technology that would allow the determination of cellular phone locations within a half second. The industry said that the plan overstepped the authority given to the FBI in a 1994 law that modernized telecommunications law enforcement technology.

    - In 1995, a group of law enforcement, defense, and intelligence agencies proposed the creation of a computer program to screen the records of 700,000 or more electronic funds transfers involving U.S. institutions and flag suspicious transactions for further investigation.

- The use of federal telephone wiretaps has increased markedly during recent years: from 340 in 1992 to 672 in 1995.

- Legislation proposed in 1996 to combat terrorism allowed the expansion of "roving" or "multipoint" wiretapping, a procedure that allows the government to tap lines besides the home and office lines used by suspects. The removal of the current safeguard (allowing multipoint wiretaps only if the suspect uses multiple phone lines in an effort to evade surveillance) could give the government access to conversations unrelated to the matter under investigation.

- **Privatization of Background Checks.** In 1996, OPM eliminated 700 jobs by making the employees responsible for background checks in several federal agencies members of an employee-owned private enterprise. At the end of three years, the contracted services would be opened to a bidding process including other private firms. Critics charge that there are inadequate safeguards in the privatization of background checks. (DEA and Customs currently contract out background checks as well.)

- **Federal Databases.** Proposals for the creation of new federal databases to track crime and immigration, similar to the National Directory of New Hires, could be a step on the way to the creation of a National Identification Card, warns Robert Ellis Smith, publisher of the *Privacy Journal.*

- **"Smart" Highways.** Automated toll collection, weight monitoring, photographing of license plates, and other measures are often undertaken without proper safeguards on the use of collected information.

- **Alleged EPA Leak.** In 1995, an EPA employee might have leaked a document about an individual involved in a property-rights case to the Sierra Club for the purpose of casting aspersions on the individual's claims.

- **Measures to Combat Food Stamp Fraud.** In response to claims of food stamp fraud, there were proposals in 1995 that would have required retailers to supply considerable additional information (such as income-tax returns) to the Department of Agriculture as a condition for participation in the food stamp program.

- **SEC.** The SEC reveals Social Security numbers provided voluntarily on certain forms contained in its online "Edgar" database.

- **Home Addresses of Federal Employees.** In 1996, after federal government shutdowns made it difficult for union representatives to communicate with federal employees, OPM decided to turn over the home addresses of its employees to federal unions.

- **Child Support Enforcement.** Vigorous measures to combat non-payment of child support, such as tracking of employee records, utility bills, and professional licenses, are underway in states such as Maryland.

Sally, Vet for privacy

EW

DRAFT EXECUTIVE ORDER

Introduction

As the largest collector and user of information on individuals, the Federal government has an obligation to set the standard for personal privacy, that is, the protection and equitable management of personal information. The *Principles for Providing and Using Personal Information* issued by the Information Infrastructure Task Force are a critical step in ensuring that our National Information Infrastructure and, indeed, the Global Information Infrastructure are transparent to all users and do not present a threat to personal privacy.

Moreover, the rapid growth of the service and information sectors of our economy, coupled with the ever-increasing capacity and versatility of telecommunications and data storage and management technology, has moved personal privacy to the forefront of consumer concerns. The *Federal Privacy Principles* propose a set of fundamental standards for maintaining personal privacy in the modern marketplace. The *Principles* may be summarized as follows:

I. *Notice* -- explain in understandable language why information is being collected, what will be done with it, and who will have access to it;

II. *Choice* -- ask only for information pertinent to the transaction at hand and do not use or sell it for other purposes without permission;

III. *Access* -- allow individuals to see information held on them on request; and,

IV. *Integrity* -- assure that personal information is secure from unauthorized access and provide a reasonably convenient and uncomplicated way to correct errors and/or include explanations.

These Federal Privacy Principles are designed to balance the rights of individuals with the information needs of both government and industry. They establish basic requirements for Federal agency privacy policies. They also serve as a means of focusing future debate on national and international standards for personal data protection.

As a first step in bringing current agency policy and practice in line with the Federal Privacy Principles, I am amending Executive Order 12160, *The Consumer's Executive Order*, to add privacy policy to the range of consumer policy issues it covers. I am instructing the Office of Management and Budget to prepare, in conjunction with the the Chairperson of the Consumer Affairs and Privacy Council established under this Executive Order, a circular to all Federal agencies directing them to modify their information management systems to incorporate these Principles and to ensure that legislative proposals submitted to Congress by the Executive Branch embody these basic tenets. I encourage State and local governments officials and business leaders to develop and implement information management systems that recognize the rights and responsibilities set forth in the Federal Privacy Principles.

To oversee adoption and implementation of these Principles, I am adding consumer privacy policy to the oversight functions of the Consumer Affairs Council which is retitled the Consumer Affairs and Privacy Council and adding consumer privacy policy to the duties and reponsibilities the U.S. Office of Consumer Affairs.

1-1. *Establishment of the Consumer Affairs and Privacy Council.*

1-101. The Consumer Affairs Council established by EO 12160 is hereby reestablished as the Consumer Affairs and Privacy Council (hereinafter referred to as the "Council").

1-102. The Council shall consist of representatives of the following agencies, and such other officers or employees of the United States as the President may designate as members:

(a) Department of Agriculture
(b) Department of Commerce
(c) Department of Defense
(d) Department of Education
(e) Department of Energy
(f) Department of Health and human Services
(g) Department of Housing and Urban Development
(h) Department of the Interior
(i) Department of Justice
(j) Department of Labor
(k) Department of State
(l) Department of Transportation
(m) Department of the Treasury
(n) Department of Veterans Affairs
(o) Corporation for National Service
(p) Environmental Protection Agency
(q) Equal Employment Opportunity Commission
(r) Federal Emergency Management Agency
(s) Federal Energy Regulatory Commission
(t) General Services Administration
(u) National Archives and Records Administration
(v) Office of Personnel Management

(w) Small Business Administration
(x) Social Security Administration
(y) Tennessee Valley Authority

1-103. The following independent agencies are invited to participate:

(a) Civil Rights Commission
(b) Commodity Futures Trading Commission
(c) Consumer Product Safety Commission
(d) Federal Communications Commission
(e) Federal Deposit Insurance Corporation
(f) Federal Emergency Management Agency
(g) Federal Maritime Commission
(h) Federal Reserve System
(i) Federal Trade Commission
(j) International Trade Commission
(k) Merit Systems Protection Board
(l) National Commission on Libraries and Information Science
(m) National Council on Disability
(n) National Credit Union Administration
(o) Nuclear Regulatory Commission
(p) Postal Rate Commission
(q) Securities and Exchange Commission
(r) U.S. Postal Service

1-2. *Functions of the Council.*

1-201. The Council shall provide leadership and coordination to insure that that agency consumer and privacy policies and programs are implemented effectively; and shall strive to maximize effort, promote efficiency, consistency and interagency cooperation in these areas.

1-202. The Council shall:

a. Serve as a forum in which members of the Council may present, evaluate, or review, information and recommendations concerning ongoing or prospective consumer and privacy issues generally, and the implementation of national consumer policies such as the Privacy Principles in particular;

b. Serve as a forum in which members of the Council may report on and coordinate ongoing or prospective agency plans and programs developed to promote effective application of consumer and privacy policies to their agency operations;

c. Provide comments, recommendations, and reports, as appropriate, to the President, the Office of Management and Budget, and agency heads;

d. Perform such other duties as are assigned by the President or his authorized designee, the Chairperson of the Council.

1-203. The Council is authorized to establish interagency working groups to perform such tasks as may be directed by the Council.

1-204. The Council may consult with other parties to perform its responsibilities under this order, and, at the discretion of the Council, such other parties may participate in Council working groups.

1-3. *Designation and Functions of the Chairperson.*

1-301. The Director of the U.S. Office of Consumer Affairs shall serve as chairperson of the Council (hereinafter referred to as the Chairperson).

1-302. The Chairperson shall be the presiding officer of the Council and shall determine the times when the Council shall convene.

1-303. The Chairperson shall establish such policies, definitions, procedures and standards to govern the implementation, interpretation, and application of this Order, and generally perform such functions and take such steps as are necessary or appropriate to carry out the provisions of this Order.

1-304. The Chairperson, with the assistance and advice of the Council, shall monitor the implementation by agencies and departments of consumer programs mandated by law, and Federal consumer policies, including the Federal Privacy Principles.

1-305. The Chairperson shall:

a. Advocate on behalf of consumers regarding the Federal government's consumer and privacy policies;

b. Develop a plan and procedures for adopting and implementing the Federal Privacy Principles in all executive agencies;

c. Assist Federal agencies in identifying and resolving privacy issues related to the implementation of their programs;

d. Identify and develop consumer and privacy issues for Council consideration, and encourage executive agencies to share knowledge and "best practices" in a timely and cooperative manner;

e. Coordinate the development of Federal consumer and privacy policy, plans and programs; and,

f. Coordinate United States consumer and privacy policy with international organizations and foreign governments.

1-306. The Chairperson shall, promptly after the close of the calendar year, submit to the President a full report on government-wide progress under this Order during that calendar year. In addition, the Chairperson shall evaluate, from time to time, the consumer and/or privacy programs of particular agencies and shall report to the President as appropriate. Such evaluations shall be informed by appropriate consultations with interested parties.

1-4. *Administrative Provisions*

1-401. The Chairperson shall utilize the assistance of the United States Office of Consumer Affairs in fulfilling the responsibilities assigned to the Chairperson under this Order.

1-402. To the extent permitted by law and subject to the availability of appropriations, the Office of Management and Budget, acting by and through the Chairperson, shall provide the Council such additional administrative services, funds, facilities, staff and other support services as may be necessary for the performance of its functions under this Order.

1-403. Each executive agency and department, to the extent permitted by law and subject to the availability of appropriations, shall cooperate with and provide such support as may be necessary to enable the Council and the Chairperson to perform their duties and responsibilities under this Order.

1-404. The Chairperson may invite representatives of non-Federal government agencies and business and consumer organizations to participate from time to time with the Council.

1-5. *Appointment of Chief Consumer Affairs and Privacy Officers.*

1-501. The head of each executive agency and department shall by 90 days from date of this Executive Order appoint a Chief Consumer Affairs and Privacy Officer, and shall make available sufficient resources to enable the Chief Consumer Affairs and Privacy Officer and the agency or department to administer consumer and privacy programs in a positive and effective manner.

1-502. The Chief Consumer Affairs and Privacy officers shall provide liaison for the agency or department to the Chairperson and shall coordinate and manage the consumer responsibilities of the agency or department as mandated by law and agency or department applications of the Federal Privacy Principles under the direction of the Chairperson.

1-503. Chief Consumer Affairs and Privacy Officers may appoint such Deputy Privacy Officers as they deem appropriate to carry out these responsibilities.

1-5. *Definitions.*

1-501. "Consumer" means any individual who uses, purchases, acquires, attempts to purchase or acquire, or is offered or furnished any real or personal property, tangible or intangible goods, services, or credit for personal,family or household purposes.

1-502. "Agency or "agencies" means any department or agency in the executive branch of the Federal government, except that the terms shall not include independent regulatory agencies or independent councils and commissions except as noted in subsection 1-103.

1-503. "Federal Privacy Principles" or "Principles" means the *Principles for Providing and Using Personal Information* issued by the Information Infrastructure Task Force on October 23, 1995. FR Reference

1-6. *Judicial Review.*

1-601. This order is intended only to improve the internal management of the Federal government and is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees.

WILLIAM J. CLINTON
THE WHITE HOUSE,
,1997

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

Record Type: Record

To: Thomas L. Freedman/OPD/EOP, Bruce N. Reed/OPD/EOP, Elena Kagan/OPD/EOP

cc: Laura Emmett/WHO/EOP

Subject: Privacy memo

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

Summary of policy options

1. **Privacy entity**: Designate a White House policy council or OMB to increase coordination on privacy issues.

2. **Online privacy**: Continue to press for industry self-regulation - with the option for a legislative solution if self-regulation proves to be inadequate.

3. **Privacy dialogue with state and local governments**: Initiate a "privacy dialogue" with state and local governments about the privacy of personal information collected by governments. Discussion could include: state privacy laws, use of Social Security numbers, impact of new technology on definition of "public records."

4. **Public education**: Work with the private sector and non-profits to develop an advertising campaign to inform individuals about how to exercise choice with respect to the collection and dissemination of their personally identifiable information.

Areas of particular sensitivity

1. **Information about children**: Call for legislation that would specify a set of fair information principles applicable to the collection of data from children (e.g. no collection of data from children under 13 without prior parental consent).

2. **Medical records**: Call for legislation on privacy of medical records consistent with HHS report.

3. **Financial records**:

   - Call for amendments to Fair Credit Reporting Act to limit the "affiliate sharing exception." Businesses could share consumer information for marketing purposes, but not for business decisions. For example, consumer information provided to an insurance affiliate could not be used to deny a person a loan without FCRA protection.

- Authorize the Fed to write enforceable rules on inter-affiliate information sharing.

- Determine whether Justice and FTC have adequate jurisdiction and penalties to punish theft of personal financial information.

4. **Profiling**: Call for legislation that would give the FTC the authority to require " profilers" to comply with a set of fair information practices. Profilers are in the business of compiling and distributing electronic dossiers on individually identifiable consumers.

5. **Identity theft**

   - Endorse Kyl bill on identity theft, provided it addresses concerns of Treasury and Justice.

6. **Social Security Numbers**: Conduct a study that looks backward to discern "lessons learned" from social security experience and looks forward to avoid the same result with respect to new identification technologies (e.g. biometrics).

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

Thomas A. Kalil
07/08/98 10:49:31 AM

Record Type: Record

To: Mary L. Smith/OPD/EOP
cc:
Subject: Privacy memo

---- PRIVACY.J7

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

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

privacy

THE WHITE HOUSE

SARAH ROSEN
SENIOR ADVISOR
NATIONAL ECONOMIC COUNCIL
(202) 456-5386 (Tel.)
(202) 456-2223 (Fax)

TO: Roger Ballentine, Paul Weinstein, Mary Smith, Thomas Freedman, Ellen Seidman, David Medine, Alan Rhinesmith, Edward Brigham, Doug Baer, Amy Friend, Becky Burr, Joan Affleck Smith, Mark McClellan, ~~Julie Williams~~, Chris Lewis, Ken Ryder, Robert Weiner

PHONE:

FAX:

DATE:

PAGES TO FOLLOW: 8

COMMENTS:

Financial privacy issues were considered in the context of a broader NEC working group on privacy which produced recommendations announced by the Vice President last week. However, there is now interest among Senate Democrats in advancing a consumer privacy amendment to the Financial Modernization bill when it is marked up in early September. We have been asked to provide technical assistance. The attached talking points suggest the direction of the Senate interest.

A meeting to discuss this issue has been scheduled for Wednesday, Aug 5th at 4:00 pm in Rm 239 OEOB.

Please RSVP + give clearance to Sonyia on 456-5351. Thank you.

INFORMATION EXCHANGES THAT ARE NOT COVERED BY THE FCRA BECAUSE OF THE TRANSACTION OR EXPERIENCE EXCEPTION

Did you know the FCRA does not prohibit ...

- your bank from selling information about which checks you have written, the amounts and to whom?
- your credit card company from selling information on which business establishments you frequent and when?
- your doctor from selling your name and information about your sensitive medical condition to marketers?
- your book store from selling your purchasing information, including books touching on political, religious or sexual matters?
- an insurance company from selling a list of its customer who are being treated for AIDS or cancer to purveyors of known quack remedies that drain the finances, as well as destroy the shortened days of terminally ill patients?

INFORMATION USE ARGUABLY PERMITTED BY THE FCRA'S PRESCREENING PROVISIONS

- A marketer, on behalf of a mortgage broker with whom the consumer had no prior or existing relationship, could telephone a consumer and record the following message on the consumers' answering machine:

  "Mr. and Ms. Sarbanes. My name is Ann Roberts. I am with Mortgage Lending, Inc. We are working with the credit bureau to help people that have very good credit, like yourselves, consolidate their debt. My records show you have about sixty-three hundred dollars in credit card debt of which we could reduce that and if you desired cash for other uses. . . . I know that you would be pleasantly surprised at what you could save in paying off those credit cards."

  This happened recently to consumers who, not surprisingly, felt that the company had accessed their credit report without a permissible purpose.

INFORMATION EXCHANGES THAT WERE FEDERALLY PROTECTED PRIOR TO THE AFFILIATE SHARING PROVISIONS IN THE FCRA AMENDMENTS

Did you know that the FCRA specifically exempts sharing of information by affiliated companies among themselves, such as --

- an employer denying a job applicant a job because the claims records of an affiliated insurance company showed that the applicant was being treated for AIDS, cancer, by a psychiatrist. In fact, under those circumstances, the applicant would be entitled to no adverse action notice and no opportunity to see and correct the information.

- credit card issuer gets a credit report on customers for account "review" purposes, passes to its lender affiliates the names of consumers that have many big balance trade lines, so the lender can solicit those consumers for a consolidation loan.

- telemarketers using "affiliate shared" credit reports, obtained because another affiliate had a clear permissible purpose to obtain the report could then call:

  -- elderly consumers who are retired on a fixed income on behalf of a brokerage house and market risky securities;

  -- minority consumers who are close to paying off their mortgage and offering them home equity loans to consolidate their high interest credit card debt;

  -- wealthy consumers, letting them know their high credit limits suggest they are the kinds of people who might be interested in a platinum card;

  -- low income consumers who could be told that due to the many negative items on their credit report, they would make excellent candidates for a secured credit card.

PROTECTING AMERICANS' PRIVACY IN THE INFORMATION AGE: AN ELECTRONIC BILL OF RIGHTS

"Privacy is a basic American value -- in the Information Age, and in every age. And it must be protected. We need an electronic bill of rights for this electronic age. You should have the right to choose whether your personal information is disclosed; you should have the right to know how, when, and how much of that information is being used; and you should have the right to see it yourself, to know if it's accurate."

-- *Vice President Gore*

In a major address at New York University this May, Vice President Gore called for an Electronic Bill of Rights to protect one of the oldest and most basic American values -- privacy -- with the rise of new technology. Today at the White House, the Vice President will announce a series of measures that represent the latest step toward making the core principles of the Electronic Bill of Rights a reality. His plan calls on everyone to do their part to protect individual privacy -- relying on private sector leadership where possible, legislation when necessary, responsible government handling of personal information, and an informed public.

The Vice President will announce new action in four key areas:

- **Protecting sensitive personal information.** Taking new executive action and calling for tough new legislation to protect personal information such as medical and financial records -- and ensuring that existing privacy statutes are strong enough to protect privacy as technology grows and changes;

- **Stopping identity theft.** Calling for strong new penalties for so-called "identity theft";

- **Protecting children's privacy on-line.** Calling for strong new measures to protect children's privacy on-line -- by ensuring that data is not collected from children without their parents' consent;

- **Urging voluntary private sector action to protect privacy.** Challenging the private sector to continue to take effective voluntary steps to protect privacy on-line.

Sensitive Personal Information

Medical Records. Currently, Americans have stronger privacy protections for their video rentals than they do for their medical records. The Administration believes this is unacceptable. The Administration has proposed strong medical privacy recommendations and urged Congress to pass legislation that gives Americans the privacy protections they need. If Congress does not pass strong medical privacy legislation, the Administration fully intends to implement privacy protections consistent with the authority given to us by the law. For example, next week the Administration is releasing a proposed rule to establish standards for the security of health information used by health care providers, health plans, and others (e.g. security and confidentiality practices, access controls, audit trails, physical security, protection of remote access points, etc.)

In 1996 Congress directed HHS to develop standards for unique health identifiers under the Health Insurance Portability and Accountability Act of 1996. However, because the availability of these identifiers without strong privacy protections in place raises serious privacy concerns, the Administration is committed to not implementing the identifiers until such protections are in place. It is also important to note that the privacy provisions passed in the House Republicans patients' rights legislation last week certainly do not pass this test, as this provision permits far too much disclosure of patient information without consent.

Financial records: The Administration will direct Treasury and the banking regulators to strengthen the enforcement of the Fair Credit Reporting Act with respect to the sharing of information between banks and their affiliates and "opt-out" notices for consumers. The Administration will also ask that Congress give bank regulators the authority to examine financial institutions for compliance with the Fair Credit Reporting Act.

Profiling: The Administration will work with the Federal Trade Commission to encourage companies that build dossiers about individuals by aggregating information from a variety of database sources to implement effective self-regulatory mechanisms. If industry attempts at self-regulation are not successful, the Administration will consider other means to ensure adequate privacy protection.

Government information: The Administration will launch a "privacy dialogue" with state and local governments. This dialogue will include considering the appropriate balance between the privacy of personal information collected by governments, the right of individuals to access public records, and First Amendment values. For example, the digitization and widespread availability of public records has raised serious privacy concerns.

Identity Theft

Identity theft: The Administration will urge the Congress to pass legislation sponsored by Senators Kyl and Leahy to crack down on "identity theft," which is the fraudulent use of another person's identity to facilitate the commission of a crime, such as credit card fraud. According to law enforcement officials, the incidence of identity theft is increasing rapidly, and current federal and state laws do not provide sufficiently comprehensive privacy protection.

Theft of personal financial information: The Administration will work with Congress to pass legislation sponsored by Representatives Leach and LaFalce that will make it a federal crime to obtain confidential customer information from a bank by fraudulent means. In some cases, people are obtaining information illegally and then using the information for a legal purpose – e.g., pretending to be a customer in order to trick confidential information out of a bank, and then selling that information to a private investigator or some other third party.

Children's Privacy

Children's privacy: The Administration will seek legislation that would specify a set of fair information principles applicable to the collection of data from children, such as a prohibition on the collection of data from children under 13 without prior parental consent. The Federal Trade Commission would have the authority to issue rules to enforce these standards. Legislation is needed because children under 13 may not understand the consequences of giving out personally identifiable information.

Calling for Private Sector Efforts

Privacy online: The Administration will continue to press for industry self regulation with enforcement mechanisms. The private sector continues to respond to the Administration's call for industry self regulation. For example, over 50 major companies and associations engaged in electronic commerce have recently created the "Online Privacy Alliance." The Administration will monitor the progress of online industry self regulation to ensure that the commitments made by companies are implemented, that the enforcement mechanisms are effective, and that the numbers of companies and organizations participating in these efforts expands so that the efforts become sufficiently broad based.

Increasing Public Awareness

Public education: The Administration will work with the private sector, the privacy and consumer advocacy communities, and non-profit organizations to develop a public education campaign to inform individuals about how to exercise choice with respect to the collection and dissemination of their personally identifiable information, and about the technologies that can make that choice possible.

A Coordinated Approach

Privacy coordination: OMB will be given responsibility for coordination of privacy issues, drawing on the expertise and resources of other government agencies. This will help improve the coordination of U.S. privacy policy, which cuts across the jurisdiction of many federal agencies.

THE WHITE HOUSE

Office of the Vice President

For Immediate Release **Contact:**
Friday, July 31, 1998 **(202)**
456-7035

VICE PRESIDENT GORE ANNOUNCES NEW STEPS TOWARD AN ELECTRONIC BILL OF RIGHTS

New Efforts Will Protect Americans' in Four Key Areas

Washington, DC -- Vice President Gore announced new steps toward an Electronic Bill of Rights, an effort to protect one of the oldest and most basic American values -- privacy -- with the rise of new technology.

"We need an electronic bill of rights for this electronic age," Vice President Gore said in an event in the Roosevelt Room at the White House. "You should have the right to choose whether your personal information is disclosed; you should have the right to know how, when, and how much of that information is being used; and you should have the right to see it yourself, to know if it's accurate."

Following a major address at New York University this May, the Vice President renewed the call for an Electronic Bill of Rights by asking everyone to do their part to protect individual privacy -- relying on private sector leadership where possible, on legislation when necessary, on responsible government handling of personal information, and on an informed public.

The Vice President announced new action in four key areas:

- **Protecting sensitive personal information.** Taking new executive action and calling for tough new legislation to protect personal information such as medical and financial records -- and ensuring that existing privacy laws are strong enough to protect privacy as technology grows and changes;

- **Stopping identity theft.** Calling for strong new penalties for so-called "identity theft";

- **Protecting children's privacy on-line.** Calling for strong new measures to protect children's privacy on-line -- by ensuring that data is not collected from children without their parents' consent; and

- **Urging voluntary private sector action to protect privacy.** Challenging the private sector to continue to take effective voluntary steps to protect privacy on-line.

###