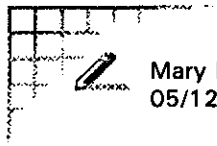
NLWJC - Kagan

DPC - Box 008 - Folder 013

Consumer Safety - Right to Privacy [2]

Const pro -
right to privacy



Mary L. Smith
05/12/98 07:09:46 PM

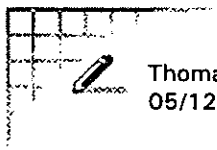
Record Type: Record

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

cc: Laura Emmett/WHO/EOP, Thomas L. Freedman/OPD/EOP
Subject: Draft Privacy Executive Memorandum

Below is a draft privacy executive memo that the VP plans on announcing on Thursday. The memo basically directs the agencies to do what they are already supposed to be doing pursuant to the Privacy Act. More specifically, the memo (1) establishes a policy on privacy throughout the federal government; (2) has agencies review their use of the Privacy Act procedures, particularly the "routine use" exemption which allows the information to be disseminated; and (3) provides for OMB to do a report on privacy within the federal government.

---------- Forwarded by Mary L. Smith/OPD/EOP on 05/12/98 06:31 PM ----------



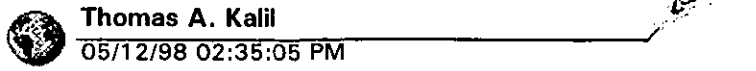
Thomas L. Freedman
05/12/98 06:15:30 PM

Record Type: Record

To: Mary L. Smith/OPD/EOP

cc:
Subject: Draft Privacy Executive Memorandum

---------- Forwarded by Thomas L. Freedman/OPD/EOP on 05/12/98 06:17 PM ----------



Thomas A. Kalil
05/12/98 02:35:05 PM

Record Type: Record

To: Thomas L. Freedman/OPD/EOP, Mickey Ibarra/WHO/EOP, Phillip Caplan/WHO/EOP, John Podesta/WHO/EOP

cc:
Subject: Draft Privacy Executive Memorandum

This still has to be circulated to the agencies -- but since we are trying to get this signed tomorrow - I thought people shold take a look at it today.

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Privacy

Privacy is a cherished American value, closely linked to our concepts of personal freedom and well-being. At the same time, fundamental principles like the First Amendment, perhaps the most important hallmark of American democracy, protect the free flow of information in our society.

The government's collection of appropriate information about its activities and about the activities of its citizens is necessary to allow it to carry out its diverse missions mandated by the Constitution. Long mindful of the potential for misuse of Federal records on individuals, the United States has adopted a comprehensive approach to limiting the government's collection, use and disclosure of personal information. Among the protections afforded information is the Privacy Act of 1974 and the *Principles for Providing and Using Personal Information*, published in 1995.

Increased computerization of Federal records permits this data to be used and analyzed in new ways that could diminish individual privacy in the absence of data protection safeguards. As development and implementation of new information technologies creates new possibilities for the management of personal information, it is appropriate to reexamine the Federal Government's contribution to accommodating the interests of a democratic society in the free flow of information and personal privacy.

Accordingly, I hereby direct executive agency heads, as follows:

Section 1. Policy.

It shall be the policy of the executive branch that agencies shall:

(a) ensure that new information technologies enhance, and do not erode, the protections of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, the Paperwork Reduction Act, and all other statutes relating to agency use, collection and disclosure of personal information;

(1) As used in this order, "agency" and "agencies" shall be defined in accordance with the definition set forth in 5 U.S.C. 552(f);

(b) assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in Section (e) of the Privacy Act of 1974;

(c) assure that all personally identifiable information not covered by the

Privacy Act be handled in a manner consistent with the *Principles for Providing and Using Personal Information* (Privacy Principles) to the extent permitted by law;

(d) evaluate new legislation and legislative proposals involving collection, use and disclosure of personal information by the Federal government for consistency with the Privacy Act of 1974.

(e) evaluate new legislation and legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles.

Section 2. Responsibilities of Agency Heads.

All agency heads shall:

(a) within 30 days, designate a senior official within the agency to assume primary responsibility for privacy policy;

(b) within one year of the date of this directive, conduct a thorough review of its Privacy Act systems of records in accordance with instructions to be issued. Agencies shall, in particular:

(1) review systems of records notices for accuracy and completeness, paying special attention to changes in technology, function, and organization that may have made the notices out-of-date, including its routine use disclosures under 5 U.S.C. 552a(b)(3) to ensure they continue to be necessary and compatible with the purpose for which the information was collected;

(2) identify any systems of records that may not have been described in a published notice, paying special attention to Internet and other electronic communications activities that may involve the collection, use or disclosure of personal information;

(c) where appropriate, promptly publish notice in the *Federal Register* to add or amend any systems of records, in accordance with the procedures in OMB Circular A-130, Appendix I;

(d) conduct a review of agency practices regarding collection or disclosure of personal information between the agency and State, local, and tribal governments in accordance with instructions to be issued by OMB;

(e) within one year of the date of this directive report to the Office of Management

and Budget on the results of the foregoing reviews in accordance with instructions to be issued by OMB.

Section 3. Responsibilities of the Office of Management and Budget.

The Director of the Office of Management and Budget shall:

(a) within <X days>, issue instructions to heads of agencies on conducting and reporting on the reviews required by Section 2;

(b) after considering the agency reports required by Section 2 of this directive, issue a summary of the results of the agency reports;

(c) issue guidance on agency disclosure of personal information via the routine use exception to the Privacy Act (5 U.S.C. 552a(b)(3)), including sharing of data by agencies with State, local and tribal governments.

Section 4. Judicial Review.

This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies, or instrumentalities, its officer or employees, or any other person.

William J. Clinton

THE WHITE HOUSE
May 14, 1998

Const pro-right to privacy

THE CLINTON-GORE ADMINISTRATION: PROTECTING OUR PRIVACY IN THE 21ST CENTURY

May 14, 1998

Today, Vice President Gore speaks at New York University's commencement. In his remarks, the Vice President announces that the Clinton Administration is proposing a comprehensive privacy action plan that will give people more control over their own personal information.

A COMPREHENSIVE PRIVACY PLAN. As technology becomes more sophisticated, the risk people face from the disclosure of personal and confidential information grows. Computers and the Internet are tools which aid us in our everyday life, but can also be used by those who wish to gain private information about us. The Clinton Administration's privacy action plan calls for:

- Legislation restricting how individual medical records are disclosed and how people can find out about their use,
- The launch of an "opt-out" Web site which would allow individuals to prevent personal information from being passed to others;
- A "privacy summit" which will include members of the Administration and industry officials, who will discuss privacy issues on the Internet.

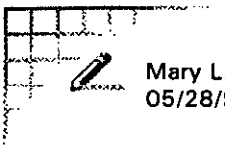
PROTECTING MEDICAL PRIVACY. The Administration will submit legislation to Congress which restricts how and when individuals' medical records can be used, gives people the right to be informed about their records, and allows them the opportunity to correct their records.

ONE STOP OPT-OUT. The Administration's plan creates a Website sponsored by the Federal Trade Commission which will enable individuals to prohibit companies from pre-screening their credit records without their permission, prevent drivers license data from being sold to data miners, and allow individuals to have their names and addresses removed from data-mailing and telemarketing lists.

ENSURING APPROPRIATE USE OF FEDERAL GOVERNMENT DATA. The President has signed a Memorandum to agency heads, effective today, that requires federal agencies to ensure that new technologies do not erode Privacy Act protections while also examining how new technologies can be used to enhance personal privacy. It also calls for a thorough agency-by-agency review of existing privacy practices, and directs the Office of Management and Budget to conduct a review and issue guidance ways agencies can protect privacy information, especially when they collaborate with state and local governments.

PRIVACY SUMMIT. To fully understand and address the complex issues involved with privacy in the Information Age, the Commerce Department will convene a Summit on Privacy to bring privacy and consumer advocates together with industry officials to explore the feasibility and limitations of the application of self regulation to the Internet and to focus on children's privacy.

Cons pro-right to privacy



Mary L. Smith
05/28/98 11:40:35 AM

Record Type: Record

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

cc: Laura Emmett/WHO/EOP
Subject: Privacy Meeting Update

Here is an update on what happened in the privacy meeting:

Sally asked that everyone come up with a draft package of privacy initiatives in two weeks. The topics that the package will address are: (1) the privacy entity in the EOP; (2) identity theft; (3) profiling; and (4) industry self-regulation (what Ira Magaziner is working on). The package will hopefully also include some legislation we could endorse.

The following are some upcoming dates:

June 4 - the industry is thinking of having a pre-announcement of how it will regulate itself
June 4 - FTC is releasing a report on privacy
June 23 - Commerce Department "summit"
July 1 -Commerce Department report to the President - Sally pushed Ira on the industry self-regulation part -- if the industry doesn't come up with a strong enough proposal, we need to have a Plan "B" to announce on July 1.

Cons pro - right to privacy

11:00

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.

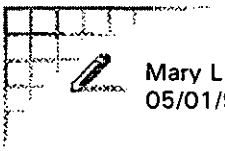
2. **Discussion of privacy entity**

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.

Civil Pro - Right to Privacy



Mary L. Smith
05/01/98 02:52:14 PM

Record Type: Record

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

cc: Laura Emmett/WHO/EOP, Christopher C. Jennings/OPD/EOP, Sarah A. Bianchi/OPD/EOP
Subject: Summary of Privacy Meeting

At the privacy meeting today, we discussed the following three topics (1) privacy entity within the government; (2) industry self-regulation; and (3) other areas the Government should take a look at such as medical records, children, etc. The decisions in these three areas would be presented as the Administration's privacy package.

(1) Privacy entity. They seem to be steering toward having the privacy entity in OMB or some EOP office like NEC or DPC. The discussion focused more on having the entity within OMB and having contact people at the agencies to deal with specific issues, particularly those that concern consumers. OMB's role would focus more on coordinating privacy policy within the Government.

(2) Industry self-regulation. Ira Magaziner talked about the developments of a consortium of businesses who would agree to post a seal on their websites, indicating that they protect users' privacy. There is envisioned to be enforcement mechanisms for misusing the seal such as existing procedures at the FTC or DOJ. The Government is expected to make a statement generally supportive of the consortium's efforts on July 1, but we would encourage more businesses to join and to go even further in thinking about specific issues such as children's privacy. In the event that the consortium doesn't seem to be making progress, Secretary Daley and Magaziner are going to explore other options such as legislation.

(3) Exploring other areas. We are also going to explore to see what, if any, position the Administration should take in areas such as medical records, genetic, financial, and children. In addition, there is going to be an exploration of "profiling" -- the amassing of information about an individual via his or her social security number and whether we should propose tighter limits on the use of social security numbers by non-government entities.

Cuts pro-right to privacy

Katzen's formulation for privacy entity.

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.

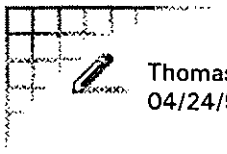
Ombudsman — Provide case-by-case assistance to consumers or businesses in resolving particular problems or complaints.

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.

Cruz pro-right to privacy



Thomas L. Freedman
04/24/98 08:10:38 PM

Record Type: Record

To: Elena Kagan/OPD/EOP, Christopher C. Jennings/OPD/EOP

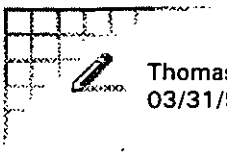
cc: Sarah A. Bianchi/OPD/EOP, Mary L. Smith/OPD/EOP, Laura Emmett/WHO/EOP
Subject: Privacy Update

You both missed another exciting privacy meeting, but don't worry Sally wants to do another one Tuesday. The main substantive issue to look forward to at that meeting is a discussion of where a possible "privacy entity" organizationally it might be placed. In the past her staff has mentioned NEC, DPC or OMB. We should talk about what the DPC position is at our Monday team leaders meeting.

The meeting today consisted of the agencies (Commerce, DOJ, HHS, Treasury) discussing what functions they thought a privacy entity should fulfill. The agencies were intitially split over what functions an entity should occupy (in the previous paper Sally circulated to you all she mentioned five possible activities -- representational, advisory, coordination, consumer advocacy, ombudsman.) Then Sally circulated the OMB recommendation which I have sent around. It suggests a representational, advisory, and coordinating role and briefly defines what they mean.

There wasn't any real discussion of health privacy issues.

Cons pro - right to privacy



Thomas L. Freedman
03/31/98 11:46:21 AM

Record Type: Record

To: Bruce N. Reed/OPD/EOP, Elena Kagan/OPD/EOP, Christopher C. Jennings/OPD/EOP

cc: Sarah A. Bianchi/OPD/EOP, Mary L. Smith/OPD/EOP, Laura Emmett/WHO/EOP
Subject: OMB/Commerce draft Privacy entity memo

PRIVACY.3

We've had preliminary meetings with the NEC/Commerce/Treasury/OMB/Commerce working group on privacy. The issues were broken down into: evaluating creation of a privacy entity in the federal government, creating a consumer bill of rights, specific initiatives on medical records and genetic privacy, internet commerce, medical records, genetic privacy, creating privacy principles, and E.U.-US trade issues.

The attached is a draft memo by OMB and Commerce on evaluating creation of a governmental privacy entity which is being pushed by Sally. The memo will go out to career agency types for comment from Commerce/OMB.

The memo lists 7 possible functions of the proposed entity and gives a recommendation. As you can see, the blander functions -- such as representing the US in trade matters and coordinating governmental policy -- are the ones the agencies have had an easier time agreeing to. I think it needs to be beefed up so that the entity is created with some explicit goal (even though it is not regulatory) that includes helping to ensure privacy, and we've asked Treasury to report back on consumer bill of right principles and their evaluation of the pending legislation in the area to see if they would support any of it.

Clinton Pro-Right to Privacy

April 8, 1998

MEMORANDUM FOR NEC DEPUTIES

FROM: SALLY KATZEN

SUBJECT: WEDNESDAY DEPUTIES MEETING

As promised, we will be devoting this meeting to a discussion of privacy issues. Attached is a quick overview of the many different aspects of the issue, from creating a governmental entity with privacy as its principal portfolio to responding to the European Union directive on the transborder flow of information.

The meeting will be **April 8** at **1:00** in room **180**. If you have any questions or need more information, please call Shannon at 456-2800.

THE WHITE HOUSE

WASHINGTON

April 7, 1998

MEMORANDUM FOR NEC/DPC DEPUTIES

FROM SALLY KATZEN, TOM KALIL

RE: PRIVACY IN THE INFORMATION AGE

I. What's the problem?

In recent years, Americans have become increasingly concerned about their privacy. In a recent Louis Harris poll, eight out of ten Americans surveyed agreed that "consumers have lost all control over how personal information about them is circulated and used by companies." Earlier this year, a three-part, front page *Washington Post* series highlighted a number of examples of the growing erosion of personal privacy, including sales by state governments of personal information.

Clearly, new technologies have made it easier to create, manipulate, store, transmit, and link digital personally identifiable information. People may disclose personal information about themselves as they travel, fill a prescription at the drug store, visit a Web site, call a 1-800 number, send an e-mail, use a credit card, or purchase groceries using a discount card. Information about these individual transactions may be bought and sold - and companies are now assembling giant "data warehouses" that contain electronic dossiers on the needs, lifestyles, and spending habits of millions of Americans.

Concerns about the loss of privacy are not just hypothetical:

- Early this year, the Navy began discharge proceedings against a sailor (McVeigh) on the basis of personal information he disclosed on America Online. The Navy investigator was able to get AOL to disclose information that linked Mr.McVeigh's screen name to his real identity.

- The drug store CVS and Giant Food recently admitted that they were disclosing patient prescription records to a direct mail and pharmaceutical company to track customers who don't refill prescriptions.

- Beverly Dennis, a women in Massillion, Ohio, received a 12-page letter containing an intimately threatening sexual fantasy from a stranger who knew her birthday, the names of her favorite magazines, the fact that she was divorced, and the kind of soap she used in the shower. The letter was written by a convicted rapist serving time in a Texas state

prison, who had been entering information for Metromail, a direct marketing firm with detailed databases on more than 90 percent of American households. Dennis' suit disclosed that Metromail had 900 pieces of information on her going back to 1987, including not only her income, marital status, hobbies, ailments, but whether she had dentures, the brands of antacid tablets she had taken, and how often she had used room deodorizers, sleeping aids, and hemorrhoid remedies.

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, and an investigatory press. For example:

- When information is true and obtained lawfully, the Supreme Court has repeatedly ruled that the state may not restrict its publication without showing a narrowly tailored and compelling governmental interest.

- Although the widespread adoption of strong encryption would increase privacy, the U.S. has maintained export controls against unbreakable encryption because of national security and law enforcement concerns.

- While the Administration believes that it is critical to protect the confidentiality of medical records, law enforcement often needs access to these records to solve crimes.

- There are significant commercial advantages that flow from the collection of personally identifiable information. As privacy expert Fred Cate put it, "Instant credit, better targeted mass mailings, lower insurance rates, faster service when ordering merchandise by telephone, special recognition for frequent travelers, and countless other benefits come only at the expense of some degree of privacy."

II. What is the current U.S. legal regime?

The U.S. has no comprehensive privacy law. Instead, the United States has a series of laws that often cover a specific industry or economic sector, or a specific use of some class of data. Many of these laws are significantly qualified by exemptions. Current statutes cover areas such as: the federal government's collection of personal information; "matching" of computerized federal records; consumer credit reports; driver's records; interception and disclosure of electronic communications; video tape rentals and sales; telecommunications services; and educational records. There are in addition a variety of state laws that take very different approaches on privacy.

Critics of the U.S. approach believe that it results in a "patchwork of uneven, inconsistent, and often irrational privacy protection ... information about a person's video rentals receives considerable statutory protection; information about medical condition and treatment does not." Defenders believe that a sectoral approach makes sense because it is difficult to

develop a "one size fits all" policy -- given the different risks involved in the disclosure of personal information and the different interests that need to be balanced.

III. What is current Administration policy?

Privacy principles

In 1995, the Administration, as part of its "National Information Infrastructure" initiative, released its "Principles for Providing and Using Personal Information." The Privacy Principles are designed to apply to the collection and use of information by both government and industry, and draw on existing international fair information practices such as the OECD guidelines.

The Privacy Principles call on those who gather and use personal information to recognize and respect the privacy interest that individuals have in personal information by (1) assessing the impact on privacy in deciding whether to obtain or use personal information; and, (2) obtaining and keeping only information that could be reasonably expected to support current or planned activities. Data gatherers should use the information only for those current or planned activities or for compatible purposes.

Because individuals need to be able to make informed decisions about providing personal information, the organizations that collect information should disclose: (1) why they are collecting the information; (2) for what purposes they expect to use the information; (3) what steps will be taken to protect the confidentiality, quality and integrity of information collected; (4) the consequences of providing or withholding information; and (5) any rights of redress that are available to individuals for wrongful or inaccurate disclosure of their information.

In July 1997, the President released the Administration's "Framework for Global Electronic Commerce." The Framework stated that the "private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy." The Secretary of Commerce must report to the President in July 1998 on the progress that has been made on industry self-regulation to protect privacy.

Sectoral policy

It is not the Administration's position that industry self-regulation is adequate in all instances. For example, on September 1997, HHS Secretary Shalala called for federal legislation on medical records consistent with the following principles:

- A prohibition on the disclosure of patient-identifiable information except as authorized by the patient or as explicitly permitted by the legislation (exceptions for public health, research, law enforcement, and oversight of the health care system).

- Provide consumers with significant new rights to be informed about how their health information will be used and who has seen that information.

- Punishment for those who misuse personal health information and redress for people who are harmed by its misuse.

In 1996, the President signed legislation that strengthened the Fair Credit Reporting Act. This legislation requires banks or other entities that report information to credit reporting agencies to:

- Not furnish information that it knows, or consciously avoids knowing, is inaccurate;

- Not furnish information whose accuracy has been disputed by a consumer;

- Promptly notify the credit reporting agency if it has provided inaccurate information and supply the needed corrections;

- In the event that there is a dispute between a consumer and a credit reporting agency with regard to the completeness or accuracy of any information furnished by the bank or other entity, conduct an investigation, review information submitted by the consumer, and report the results of the investigation to the relevant agency and, if the furnished information proved to be inaccurate, any other agency that received the information.

IV. What is the U.S.-EU dimension of the privacy issue?

The EU has adopted a Directive on Data Protection, which becomes effective in October 1998. One provision of the Directive prohibits transfer of personal information to other countries that lack "adequate" protection of privacy. If the EU were to rule that the U.S. does not provide "adequate protection" of privacy - it could significantly reduce the flow of data between the U.S. and Europe and disrupt trade and the operations of U.S. firms doing business in Europe.

The EU Directive is different from the U.S. approach because it:

- Covers all sectors and is extraordinarily broad;

- Requires that anyone that is processing personal data register with national authorities before beginning any data processing; and

- Requires member states to establish an independent public authority that can wield investigatory powers, hear complaints, order the cessation of data processing activities, block the transfer of data to third parties, and impose penalties.

Some analysts believe that the EU Directive is so broad that it will make routine behavior

illegal (e.g. a salesperson who enters names on a laptop without someone's unambiguous consent and leaves the country) -- and that the EU can not possibly enforce the letter of the law.

It is not yet clear whether the EU would regard a U.S. industry-led initiative to strengthen privacy protection as "adequate." One of the common European criticisms of the U.S. approach of relying on self-regulation is that is "lacks teeth."

V. What are some potential options to strengthen the privacy of Americans?

Option A. **Define what effective industry self-regulation is -- promote efforts by the private sector to achieve effective self-regulation.**

The Commerce Department has developed a set of criteria for judging whether or not a self-regulatory regime is effective that it plans to publish in the *Federal Register* for comment. These criteria include support for the key fair information principles discussed above, and enforcement mechanisms, including:

- **Consumer recourse** for resolution of disputes.
- **Verification** that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented.
- **Consequences.** For self-regulation to be effective, failure to comply with fair information practices should have consequences (e.g. cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a publicly available "bad-actor" list, disqualification from membership in an industry trade association, liability for fraud).

A coalition of U.S. businesses, lead by IBM, proposes to create a self-regulatory umbrella group to promote compliance with fair information practices on the Internet that the Commerce Department believes is consistent with its principles. The group intends to "preview" the initiative in May (at the DOC privacy event), with a commitment to begin operations in September, 1998. At this point, the composition of the alliance has not gelled. We understand that AT&T, EDS, Hewlett-Packard, and a number of other businesses are in discussion with IBM.

A longer description of the private sector initiative is attached.

Option B. **Establish a "privacy entity" within the federal government.**

One criticism of the U.S. privacy policy is that there is no part of the government that has privacy as its primary mission. A privacy entity within the federal government could have a number of functions, including:

- **Representational**: Explain and promote the U.S. government position on privacy policy domestically and internationally.

- **Advisory**: Provide technical assistance to privacy policy questions raised by government agencies and by private sector entities.

- **Coordination**: Apprise appropriate government agencies of emerging privacy issues and ensure that these issues are addressed

- **Regulatory/enforcement**: Create and administer legally enforceable regimes of fair information practices including the use of some combination of inspection, registration, reporting, civil or criminal action, adjudication, and penalties. [Note that this would be inconsistent with Administration policy to date.]

- **Ombudsman**: Case-by-case assistance to consumers or businesses in resolving in response to their particular problems or complaints.

- **Education**: Provide privacy information (including model practices and "rights and responsibilities") to citizens, industry, and government.

- **Consumer Advocacy**: Monitor 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.

- **Evaluation**: A policy advocacy role (as contrasted with a consumer advocacy or ombudsman role) to give opinions, promote good ideas and practices, and scrutinize less good ones.

After deciding what functions the "privacy entity" would carry out -- the Administration would have to decide where to put it. A meeting was held earlier this year to discuss the functions of a privacy entity - and a memo that is also being sent to the privacy contacts of agencies is attached.

OPTION C. **Pursue legislative and administrative solutions for specific sectors or types of data.**

[Information to be supplied.]

Description of "Alliance for Online Consumer Awareness"
Department of Commerce, April 6, 1998

A coalition of U.S. businesses, lead by IBM, proposes to create a self-regulatory umbrella group to promote compliance with fair information practices on the Internet. The group intends to "preview" the initiative in May (at the DOC privacy event), with a commitment to begin operations in September, 1998. At this point, the composition of the alliance has not gelled. We understand that AT&T, EDS, Hewlett-Packard, and a number of other businesses are in discussion with IBM.

The alliance proposes to work with business, consumer groups and privacy advocates to create an "accountability mechanism" available to any consumer in connection with any online encounter. The organization would provide:

- support for fair information practices including awareness, choice, security, access and accuracy;[1]
- business education and encouragement of companies and associations to promulgate and post privacy guidelines and/or policies developed on sectoral basis by individual business sectors;
- consumer outreach and consumer education about privacy rights and how to protect personal privacy online;
- resolution of "legitimate" consumer complaints;
- verification, as appropriate, of business compliance with stated privacy policies;
- consequences for businesses that fail to adhere to stated practices (investigation and disclosure of noncompliance, revocation of alliance seal, referral to consumer protection agencies when complaints are not resolved through private dispute resolution mechanisms).

In addition to general support for fair information practices, the alliance proposes to

---

[1] In general, the alliance would enforce privacy policies developed on a sectoral basis. The alliance would require, however, that all policies comply with the fair information practices guidelines established by the OECD in 1980. The alliance believes that some evolutionary period will be needed, however. For example, some time may be needed to reach agreement on consumer access to their personal data.

The alliance would also require members to comply with specific rules relating to the collection of data from children. Alliance members are discussing appropriate rules governing the collection of data from children. We believe that theses rules should, at a minimum, provide the protections outlined in FTC staff guidance on the subject.

focus on consumer education (to increase awareness) and on accountability.

To promote consumer awareness and empowerment, the alliance would publish basic educational materials about online privacy. For example, the alliance would provide what they should consider before disclosing personal information. the alliance would provide training on the use of consumer empowerment technology. It would create a digital seal (like the "Good Housekeeping Seal of Approval") to encourage consumers to do business with companies that adhere to fair information practices. The alliance would also make information available about non-compliance, based on verified complaints about personal data protection practices.

To enhance business accountability for inappropriate use of personal data, the alliance would provide a hotline/hotsite to respond to consumer inquiries about online privacy and suspected violation of fair information practices. The alliance would help businesses develop privacy policies, and if a company chooses, permit a company to display an alliance seal that assures consumers that a particular online business complies with fair information practices. The alliance would audit or otherwise assess member company compliance.[2] Finally, the alliance would handle consumer complaints about privacy violations.

The coalition is currently discussing a partnership with BBBOnLine, a subsidiary of the national Council of Better Business Bureaus. Under this model, BBBOnLine would provide a competitor challenge and consumer complaint resolution service, including mediation and arbitration using the existing BBB dispute settlement apparatus.

The alliance is also current discussing a partnership with TRUSTe, an organization that provides trust marks (seals), backed by independent audits and third party verification (list seeding, etc.).

The details of the alliance proposal are still under discussion with founding members. The proposal appears, however, to have the elements that we believe are necessary to create effective self-regulation for privacy.

---

[2] The use of independent audits and/or other independent assessment mechanisms remains controversial. Traditional financial audits are quite expensive and may not be necessary in all cases. While we are willing to consider other approaches, we believe that independent assessment of adherence with fair information practices is a critical element of any self-regulatory approach to data privacy.

Attachment to Memorandum to Privacy Contacts

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.

Attachment to Memorandum to Privacy Contacts

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.

Attachment to Memorandum to Privacy Contacts

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."

Cms pro-Rt to Privacy

April 8, 1998

MEMORANDUM FOR NEC DEPUTIES

FROM: SALLY KATZEN

SUBJECT: WEDNESDAY DEPUTIES MEETING

As promised, we will be devoting this meeting to a discussion of privacy issues. Attached is a quick overview of the many different aspects of the issue, from creating a governmental entity with privacy as its principal portfolio to responding to the European Union directive on the transborder flow of information.

The meeting will be **April 8** at **1:00** in room **180**. If you have any questions or need more information, please call Shannon at 456-2800.

* Additional Info.

MEMORANDUM

4/7/98

TO: Tom Kalil

FROM: Becky Burr

RE: Legislative/Regulatory Approaches to Privacy

We believe that public concern with respect to privacy 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.

At your request, I have reviewed privacy related legislative proposals introduced in the 105th Congress. In addition, the Department of Commerce has several recommendations regarding regulatory and/or executive steps that could be undertaken to enhance privacy protection.

LEGISLATIVE APPROACHES

Legislative proposals fall into one of several broad categories: 1) medical records, 2) genetic privacy and non-discrimination, 3) use of social security numbers by government and business, 4) information relating to children, and 5) online privacy. Many of the proposals address important issues. For the most part, however, the legislative proposals have been introduced in reaction to a particular high-profile privacy horror story. They tend to be reactive, and not particularly well though out. As a result, the Administration would want to seek at least some modification of any of the proposals prior to endorsing them.

This memo does not address privacy proposals related to encryption policy.

Medical Records

The Clinton Administration has called for legislation to protect the privacy of medical records, and may want to enforce this position by supporting specific legislation.

Senators Leahy and Kennedy introduced S.1368, the Medical Information Privacy and Security Act, in November. This is a general medical privacy bill, and is viewed positively by the advocacy community. The bill outlines certain individual rights to medical records, including access rights. S 1368 requires specified parties to establish safeguards to ensure the

confidentiality, security, accuracy and integrity of protected health information based on model safeguard guidelines. The legislation would prohibit the unauthorized release of protected medical records except under limited circumstances. The bill would also establish an Office of Health Information Privacy at HHS to investigate complaints and conduct audits. This legislation generally follows the HHS recommendations, but provides more limited law enforcement access (requires court order). The research community has concerns about some aspects of this bill, but the sponsors have indicated flexibility in this area.

Senator Jeffords has also introduced medical records legislation, which is viewed with less enthusiasm in the advocacy community but may be more acceptable to the pharmaceutical industry. This is designed to be much less onerous than the HHS recommendations. Senator Boxer has introduced S. 1499, the Health Insurance Consumer's Bill of Rights Act of 1997, designed to enhance medical records privacy in the managed care industry. In the House, Rep. Condit introduced HR 52, the Fair Health Information Practices Act, to establish a code of fair information practices for health information.

Genetic Information

Several bills have been introduced to limit disclosure of and prohibit discrimination on the basis of genetic information. *See* HR 306 (Slaughter), HR 341 (Stearnes), HR 1815 (McDermott), HR 2216 (Kennedy), HR 2275 (Lowery), HR 3442 (Smith), S 89 (Snowe), and S 422 (Domenici). The Administration may also want to consider legislative proposals to limit the secondary using of biometric information. Legislation to protect biometric information is under consideration in California, but has not yet been introduced in Congress.

Social Security Numbers

The Administration may want to undertake a study of or consider supporting legislation that would limit the non-governmental use of social security numbers for identification purposes.

HR 1287, introduced by Rep. Franks, would prohibit interactive computer services from disclosing social security numbers without the holder's consent. Rep. Kenelly's proposal, HR 1331, requires the Commissioner of Social Security to create an experts panel to advise the Social Security Administration on how to ensure the confidentiality and integrity of SSA records made available to the public. Other proposals include HR 1813 (Kleczka), HR 2404 (Filner), HR 2581 (Campbell, T.) Rep. Kanjorski's bill, HR 1330, would prohibit federal employees from making social security information available through the Internet, and would establish a commission to investigate the protection and privacy afforded to certain government records.

Senator Feinstein has introduced S 600 (companion bill to HR 1813, Kleczka) to prohibit the commercial acquisition or distribution of an individual's social security number as well as its use as a personal identification number without the individual's written consent. The Act would

also require that State DMV use of social security numbers be consistent with the uses authorized by the Social Security Act, the Privacy Act, and any other statutes explicitly authorizing their use. The Bill would prohibit the use of social security numbers by marketing companies. The business community already uses social security numbers extensively, so this legislation is quite controversial.

Children

Bob Franks has introduced HR 1972, which prohibits list brokers from selling or purchasing information about children without written parental consent. Senator Feinstein introduced the companion bill in the Senate (S 504). The bill also prohibits the use of prison inmate labor for data processing personal information about children.

Online Privacy

A number of legislative proposals address online privacy in general.

HR 2368 (Tauzin), the Data Privacy Act, provides for the establishment of a computer interactive services industry working group to establish voluntary guidelines relating to data collection and spamming. The bill prohibits display of social security numbers online, and limits the marketing of certain government information obtained online without the data subject's consent.

HR 98 (Vento), the Consumer Internet Privacy Protection Act, prohibits computer services from disclosing personally identifiable information about a subscriber without the subscriber's prior informed written consent. The proposal authorizes the FTC to investigate violations as well as providing an individual cause of action for subscribers aggrieved by prohibited disclosures.

HR 1964 (Markey), the Communications Privacy and Consumer Empowerment Act, requires the FTC to investigate whether consumers have adequate notice about information being collected from them and a means to exercise control over and stop unauthorized use of such information. The FTC is further called up to propose changes in FTC regulations and/or recommend legislation to correct defects in privacy rights and remedies. The bill also directs the FCC to undertake a similar proceeding. The legislation does, however, prohibit the government from restricting the sale of strong encryption.

REGULATORY/EXECUTIVE APPROACHES

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

technology facilitates datamining and seamlessly creates transactional records, privacy concerns often surface in connection with the Internet. We should keep in mind, however, that existing statutory protections and regulatory obligations already apply to personally identifiable information on the Internet.

Keeping in mind that the Internet is often simply a conduit, the nature of the medium makes legislative solutions less likely to provide real privacy benefits. Given this situation, the President challenged the private sector to develop and implement effective self regulation for privacy, including codes of conduct, industry developed rules, and technological solutions to protect privacy on the Internet. Industry is beginning to take up this challenge (see memo on "Alliance" proposal).

Nonetheless, the government could act to enhance privacy in a networked environment, especially with respect to concerns about "profiling."

An enormous amount of information used to create individual profiles 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 the opportunity to choose not to make their data publically available.

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 discloses, or should the Administration begin an initiative to reduce data collection (and thereby disclosure) and urge 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? (Note, however, that this will raise significant open government/First Amendment issues.)

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) similar to the Fair Credit Reporting Act that would give consumers choice, or information at a minimum, about use of their personal data for this purpose.

Cms Pro-Right to Privacy

Food Labeling

82/10% support/oppose requiring all fruits and vegetable to be labeled to tell you if they come from within the United States or if they are imported.

82% support (24 somewhat + 58 strongly)
10% oppose (6 somewhat + 4 strongly)

Privacy

This is an issue for the introduction of new legislation/executive orders.

Technology is decreasing the amount of privacy individuals have in their daily lives.

81/16 agree/disagree.

75% think the federal government should do more to protect individual's privacy **(22% no).**

The following are some proposals people have suggested to increase people's privacy in the new information age. For each one please tell me if you strongly support...	**Strongly Support**	**Support /Oppose**
Requiring your prior permission before anyone can release your personal medical records.	87	96/4
Requiring your prior permission before anyone can release your personal financial records.	86	92/7
Prohibit internet services from disclosing an individual's Social Security Number without the individual's prior, written consent	83	90/9
Prohibit commercial acquisition of an individual's Social Security number and prohibit the use of Social Security numbers by marketing companies	77	85/14
Increase penalties for illegally intercepting cellular telephone conversations	75	87/11
Ask all internet companies to establish guidelines for the distribution of personal information such as health and medical information.	71	87/11
Require the Federal Trade Commission to determine all methods by which consumers can learn what information about them is being collected, used and sold.	69	83/14

Cum Pro - Right to Privacy

Privacy Protection in the Digital Age

There are four widely accepted principles for privacy protection based on OECD guidelines which we are seeking to put in place.

1. A person should be notified that information is being collected about them and what is intended to be done with any information that is collected.

2. The person should have the choice as to whether their information is collected and how it is used.

3. The person should have access to the information and an ability to check it for accuracy.

4. There should be adequate enforcement of these privacy protections and redress for consumers who believe their privacy has been violated.

There are certain areas such as credit and medical records where a legislative approach may be the best way to implement these principles; however, for electronic commerce in general, a legislative approach would be very difficult to enforce. Tens of thousands of web sites form every week on the Internet. No Government agency could possibly monitor them all for compliance with legislation, and consumers would often not know whether their privacy was being violated or not.

Instead, we favor a system with the following components:

1. An industry consortium with participation from consumer groups would recognize industry established sectoral codes of conduct which stipulate procedures for notice, choice, enforcement, redress and verification. Companies who sign up to these codes would join the consortium and can display a seal on their website.

2. The consortium sets up an independent secretariat with consumer group participation which conducts audits of websites displaying the seal to ensure that they are conforming to the code. They also handle consumer complaints. They can enforce the code by removing the right to display the seal from those who violate the policy, publishing the names of violators, imposing fines or if necessary referring for prosecution under existing anti-fraud or other laws those who violate the policy.

3. The Government, industry, and consumer groups can run education campaigns for consumers making clear that they are free to go wherever they wish on the internet, but that if they visit or buy from a site which does not have one of the privacy seals, their privacy may not be protected. This empowers the consumer by creating safe zones on the internet for privacy and giving them the tools to protect their own privacy.

4. New websites will have a market motivation to seek out a seal from a code of conduct organization because otherwise they will be limiting their market since many people will not visit or shop at sites without a seal.

5. The code of conduct organizations can operate internationally through cooperative agreements among private organizations so that consumers are protected globally.

6. This system allows decentralized enforcement in a non bureaucratic, flexible way and creates market mechanisms to encourage participation.

Today, there are pieces of this in place through groups like the Direct Marketing Association, Trust - e and others. There is now an effort underway to put together a code of conduct consortium of major players who make up a significant percentage of the traffic now on the Internet. If this comes together, there will be the nucleus around which to build an effective industry self regulation system. The consortium which is led by IBM is committing to have something in place by mid May and to implement in reasonably rapid stages after that.

In preparation for the NEC meeting in early April, we will describe this activity, discuss who is behind it, and give our assessments of its chances for success.

Cons. Pro - Rt to Privacy

Check Status

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

Right to
consumer protection - privacy

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.

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.

Consumer Safety - Right to Privacy

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]

The New York Times

THURSDAY, JUNE 12, 1997

Personal Files Via Computer Offer Money and Pose Threat

By NINA BERNSTEIN

It was past midnight when Beverly Dennis came home, weary from her second-shift factory job, and found a letter with a Texas postmark among the bills and circulars in the day's mail. As she read it in her small house in Massillon, Ohio, alone in the dark stare of the sliding glass doors, her curiosity turned to fear.

The letter was from a stranger who seemed to know all about her, from her birthday to the names of her favorite magazines, from the fact that she was divorced to the kind of soap she used in the shower. And he had woven these details of her private life into 12 handwritten pages of intimately threatening sexual fantasy.

"It can only be in letters at the moment," the man wrote after describing the sexual acts he planned. "Maybe later, I can get over to see you."

The explanation that eventually emerged deepened Ms. Dennis's sense of violation — and places her experience at the heart of a far-reaching national debate over legal protection for privacy in a world where personal information is ever easier to mine and market.

The letter writer was a convicted rapist and burglar serving time in a Texas state prison. He had learned Ms. Dennis's name, address and other personal information from one of the product questionnaires that she and millions of other consumers had received in the mail, innocently completed and sent back to post office boxes in Nebraska and New York on the promise of coupons and free samples. Their answers were delivered by the truckload to the Texas prison system, which was under contract to handle the surveys for the Metromail Corporation, a leading seller of direct marketing information. Hundreds of unpaid inmates, many of them sex offenders, entered the information on computer tapes for Metromail, which has a detailed data base on more than 90 percent of American households.

To Ms. Dennis, a woman in her 50's who grew up in the coal country of southern Ohio, it was as though her privacy had been strip mined by the dark side of the information economy.

Indeed, as the free-flowing exchange and exploitation of information is being celebrated as the main engine of economic prosperity into the next century, individual privacy is looking more and more like an endangered natural resource.

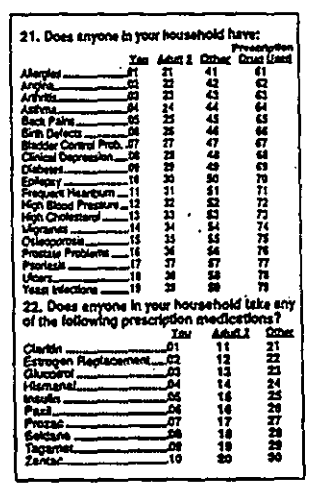
Hunger for personal information is now growing explosively in almost every sector of the nation's economy and everyday life, from health care to entertainment, from banking to supermarket sales. It is being

Continued on Page A30

LIVES ON FILE

The Erosion of Privacy

A special report.



21. Does anyone in your household have:

	You	Adult 2	Other	Prescription Drug Used
Allergies	01	21	41	61
Angina	02	22	42	62
Arthritis	03	23	43	63
Asthma	04	24	44	64
Back Pains	05	25	45	65
Birth Defects	06	26	46	66
Bladder Control Prob.	07	27	47	67
Clinical Depression	08	28	48	68
Diabetes	09	29	49	69
Epilepsy	10	30	50	70
Frequent Heartburn	11	31	51	71
High Blood Pressure	12	32	52	72
High Cholesterol	13	33	53	73
Migraines	14	34	54	74
Osteoporosis	15	35	55	75
Prostate Problems	16	36	56	76
Psoriasis	17	37	57	77
Ulcers	18	38	58	78
Yeast Infections	19	39	59	79

22. Does anyone in your household take any of the following prescription medications?

	You	Adult 2	Other
Claritin	01	11	21
Estrogen Replacement	02	12	22
Glucotrol	03	13	23
Humanal	04	14	24
Insulin	05	15	25
Paxil	06	16	26
Prozac	07	17	27
Sotalure	08	18	28
Tagamet	09	19	29
Zantac	10	20	30

A Texas woman's answers to this 77-question consumer survey ended up in the hands of felons.

spurred and sharpened by powerful market forces and ever more pervasive computer technology, including digital mapping tools and so-called "data-mining" software that blast commercial value from newly linked data bases of unprecedented size.

Yet like the people whose private lives and public records passed through the fingers of Texas felons, most Americans have no idea what is happening to the stream of personal data that they shed just by living in the modern world. And most businesses that make money on the collection, recombination and sale of shards of personal information maintain that people need no legal right to know, and have no good reason to object.

The electronic deposits keep growing with the pulse of daily life: telephone calls, checkout counters, A.T.M.'s, and electronic bridge tolls, the street gaze of security cameras, plastic insurance cards imprinted with the Social Security numbers that have become identity's common currency — and its easy counterfeit.

The Internet, where every keystroke can be archived, is now the most dramatic embodiment of what technology and commerce afford in the real world: the pooling of ever more vast stores of data, and the easy retrieval of individual specks with no one's say-so.

This networked world of information is an economic powerhouse that creates new jobs, new services and astonishing efficiencies. It offers a wide range of consumer benefits, including easy credit, shopping convenience and customized goods and services. It also turns commonplace transactions into little revelations.

When a clerk puts a supermarket discount card through the scanner, for example, a data base links the shopper's identity with the bar code on every item bought. A love of rich chocolate cookies not only can be tracked over time, but matched with an individual's address, age, weight and ethnicity, with marital status and credit standing and even with religious ties, to name just a few of the personal facts being bought and sold wholesale in today's booming information market.

A class-action lawsuit that Ms. Dennis filed last year against Metromail and its subcontractors is emblematic of the growing conflict over privacy as people learn how little they control the use of personal information that is an increasingly valuable corporate asset.

"Privacy will be to the information economy what consumer protection and product safety were to the industrial age," Marc Rotenberg, director of the Electronic Privacy Information Center in Washington, warned at Federal Trade Commission hearings on electronic consumer privacy last year. This week, the F.T.C. is holding another round of hearings on the issue.

But as Ms. Dennis has learned during a three-year struggle for redress, any battle for privacy today is an uphill fight, and individuals have an inherent disadvantage.

Ms. Dennis spent sleepless nights trying to figure out the stranger's identity. She finally turned to local television news reporters for investigative help, and searched for more than a year before she found a lawyer willing to take on a novel and demanding case without pay.

But when Metromail executives wanted to know more about the woman suing the company, their task was simple: They turned to the company's own massive consumer data base, and retrieved more than 900 tidbits of Ms. Dennis's life going back to 1987. Laid out on 25 closely printed pages of spreadsheets were not only her income, marital status, hobbies and ailments, but whether she had dentures, the brands of antacid tablets she had taken, how often she had used room deodorizers, sleeping aids and hemorrhoid remedies.

"Attached is all we know concerning Beverly Dennis," Dave Hansen, an information technology systems analyst, wrote in a May 3, 1996, memorandum circulated to top executives and the chief lawyer for Metromail, which had $281 million in revenues last year and has budgeted $1.5 million to fight the case. The memo was one of the internal documents the company was recently required to turn over to the plaintiffs under discovery rulings by a state court in Travis County, Tex.

The company dossier on Ms. Dennis illustrates a central issue in the privacy debate: Information collected in one context can be reused in entirely unanticipated and even hostile ways without the knowledge or consent of the individuals involved. United States law offers them little recourse.

The Supreme Court has recognized an unwritten right to privacy in the Constitution, but has essentially limited this right to the individual's "reasonable expectation" of privacy. That approach, privacy experts say, means the steep but silent erosion of privacy by technological and economic change keeps narrowing the right to protection that an individual can successfully claim in court as "reasonable" — especially since privacy is weighed against competing interests, like law enforcement or freedom of the press. And like the unwritten constitutional right to privacy, most of the nation's patchwork of privacy legislation aims to protect individuals from government, not from the actions of private industry.

Metromail maintains in court that it did nothing wrong and that Ms. Dennis has no reasonable claim to privacy because she disclosed the information herself in consumer surveys. The company, a leading member of the Direct Marketing Association that champions industry self-regulation, calls the case an aberration, and adds that it no longer uses prison labor.

Because of the case, Texas is considering a complete ban on data entry by prisoners, but inmates in at least 27 other states handle public records like motor vehicle registrations, and Federal prisoners do such work for the Internal Revenue Service, among other public agencies. Prisons in at least five states reported contracts to process information for private businesses.

Public records are part of Metromail's information products. Its offerings include a "Behaviorbank" line that, for 4 cents to a quarter a piece, sells names, addresses and personal characteristics of respondents like Ms. Dennis to a wide assortment of clients, from direct marketers, bill collectors and reporters to politicians. Metromail customers include the marketing departments of major magazines and newspapers, including The New York Times.

Four new plaintiffs recently joined the class action by name after their information showed up in records that the lawsuit forced from Metromail and its subcontractor, Computerized Image and Data Systems in Roslyn Heights, N.Y., which sent the work to the prisoners. Like Ms. Dennis, the new plaintiffs said they felt tricked by surveys headlined, "Spending Too Much. You Can Save Money At the Supermarket," or "No sweepstakes, no promises, no gimmicks. Just FREE coupons, samples and other special offers." The outrage they expressed goes well beyond the prisoners' access to such data.

One, Edward Boslet, a 36-year-old meatcutter turned home health care technician in Plattsburgh, N.Y., summarized what to him is the heart of the matter.

"It's my information, it's not theirs," Mr. Boslet, a father of three, said in a telephone interview. "The bottom line is, I should have a right to know. I should have a right to choose who they're going to sell it to and what list I'm going to be on. There should be some way to govern what they do."

His convictions are not so far from the principles of fair information practice adopted by the European Union. But they are far from policy or practice in the United States.

Many people, especially in business, feel that is all to the good. They credit an unrestrained market in personal information as one reason for the United States' lead in the information economy.

"It's beneficial to the economy, it's beneficial to consumers," said Chet Dalzell, a spokesman for the Direct Marketing Association, the main trade group that is a longtime proponent of letting the industry regulate itself on privacy issues. Because the market can decide how to use personal information, he said, consumers get competitive offers of goods and services that are timely and relevant to their own lives, while businesses save on marketing costs.

"This isn't a war," Mr. Dalzell added. "This is the marketplace just trying to be intelligent." A recent study that the association commissioned from Clemax-WEFA, an economics consulting company, said one of every 13 jobs in the United States is the result of direct marketing sales activity, including jobs designing and selling advertising, supplying or delivering goods, and selling other support services, like customer lists and profiles, to direct-response businesses. Direct-marketing sales to consumers reached $630 billion last year, up from $458 billion in 1991. Business-to-business sales were $540 billion in 1996, up from $349 billion in 1991, according to the Clemax-WEFA report.

In other sectors, from health care to welfare, the ever more intensive use of personal information is being embraced as a way to cut costs and improve outcome, whether through employee "wellness" plans that discourage unhealthy life styles, or through child-support enforcement programs that combine public and private sector data bases to find parents who are delinquent in child support payments.

But incidents like these across the country offer glimpses of the less visible tradeoffs:

¶At a car dealership in northern New Jersey, 15 employees used the company's access to the Big Three credit bureaus —

Equifax Inc., Trans Union and TRW Inc. — to find strangers with good credit histories, living as far away as Alaska and Washington. They opened credit accounts in the customers' names, ordered thousands of dollars in products and left the victims to struggle to restore their credit ratings. What made the 1993 case unusual was that the culprits were caught. Quick credit and ready access to Social Security numbers have made "theft of identity" one of the fastest growing forms of credit fraud, according to the U.S. Public Interest Research Group, a consumer advocacy organization. Officials at Trans Union said the credit bureau gets 45,000 to 50,000 calls a month from people complaining that their accounts have been taken over.

¶A convicted child rapist working at a Boston area hospital in 1993 was accused of using a former employee's computer password to rifle through nearly 1,000 confidential files of patients for telephone numbers he used to make obscene calls to girls as young as 8 years old. Like many hospital systems, this one neither locked out defunct passwords nor triggered a warning when one person called up an unusual number of files. In an even more startling case, reported by The New York Times last year, a convicted pedophile in a Minnesota prison was accused of compiling a computerized data base of more than 5,000 children and babies, annotated with descriptions like "cute," "latchkey kids" and "Little Miss pageant winner." The lists, apparently pieced together from items in small-town newspapers, were stored with child pornography obtained over the Internet.

¶Earlier this year, the Sara Lee Corporation asked a health maintenance company to survey and screen all 500 employees in its Mesilla Park, N.M., hosiery factory, for signs of depression that might underlie sick days and affect job performance. The plan was for the employees' personal physicians to consider prescribing antidepressants, according to an account in Fortune magazine that stressed the potential medical cost savings of the pilot project by Lovelace Health Systems, a subsidiary of the Cigna Corporation. Later, Anne Munsen, a spokeswoman for Lovelace, said the magazine account caused the project to be put on hold: the employees at the nonunion factory were not supposed to know the true purpose of the survey. "They didn't want it to be seen as a depression screening," she said, "they wanted it to be seen as a health-risk screening."

According to successive polls conducted by Louis Harris for Equifax in 1994 and 1995, 4 out of 5 Americans are concerned about threats to their personal privacy. This is a growing public relations problem for business, which has its own brand of privacy concerns: the ability to keep proprietary information "private" in a networked world competing for a data edge.

But a strong undercurrent dismisses privacy as "the ultimate subjective, touchy-feely issue," as Robert J. Posch, Jr., a vice president at Doubleday and marketing law specialist, put it. In the trade magazine Direct Marketing, he scoffed that privacy was "just some notion of the right to be left alone. Spare me."

Both legal scholars and computer scientists who advocate more privacy rights for individuals contend that in the information economy, privacy is less about seclusion than about power, and the personal autonomy necessary to democracy.

"Through the use of data banks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children," wrote Paul M. Schwartz and Joel R. Reidenberg, two American lawyers who were commissioned by the European Union to study American data privacy law and who published their critical findings in a book last year. "Companies take the position that the use of personal information is in the best interests of customers. Yet these companies deny consumers the opportunity to judge for themselves."

The Clinton Administration has called for a balance between individual privacy and the needs of an increasingly information-driven economy, but like the two previous administrations, it has made industry self-regulation the centerpiece of its privacy policy.

Critics contend that self-regulation amounts to little more than public relations, and that the titans of information are despoiling democracy's inner landscape with as little restraint as the coal barons and oil trusts showed during laissez-faire industrial growth.

Ms. Dennis's case offers a rare look at the human dimension of the conflict, and provides a road map to the hidden places along the way where gold is spun from the raw data of people's lives.

A Prison

In a Growth Industry, Inmates Process Data

In the heat-soaked shimmer of an August noon in 1996, in a field outside a Texas penitentiary, prisoners with hoes stood double file, before a lone guard on horseback. It was a tableau from an earlier era.

Okra and cotton are still raised by some of the 138,000 inmates serving time in the fifty-two prisons within the Texas Department of Criminal Justice. License plates still clatter from noisy machines manned by convicts inside the big Huntsville prison, southeast of Dallas, where visitors are given a bumper sticker that reads "Texas — It's Like Another Country." But since 1968, when a Records Conversion Facility opened at the Wynne prison unit in Huntsville, information has been part of Texas prison industries.

On this day, thousands of boxes of public records were passing through the vast, low-slung steel-frame building, one of five such prison operations in the state, and one of dozens across the country. Under hanging fluorescent lights, an acre of men in dingy prison whites turned documents from public agencies into microfilm images and computer bytes.

"Anything and everything could be in here," said DeeWayne Beckham, the assistant plant manager. At random, he picked up a record from the Bexar County courts in San Antonio. It was a petition in a 1991 divorce case asking for child support for a girl named Megan.

There were patient progress reports from the Brenham State School for the mentally disabled in Brenham, Tex., motor vehicle titles from the Texas Department of Transportation, criminal investigation records from police and the state attorney general's office. The last were stacked high behind a special wire mesh cage, for fear, Mr. Beckham said, that inmates would steal crime scene photographs and sell them.

"I've got murderers, and whatever else you can imagine," Mr. Beckham said cheerfully, passing a man with tattoos on three fingers in a group unstapling and sorting documents at a long table. Other prisoners fed the pages into microfilm machines that capture as many as 17,000 pages a day.

Nearby, inmates typed at computer keyboards, producing computer tapes from 30,000 applications for the government's Women, Infants and Children nutrition program for low-income pregnant women and young children.

This was the data-entry section where, under the unit's first and only private sector contract, inmates in three shifts handled thousands of the Metromail "Shoppermail" questionnaires each day in 1993 and 1994, as well as other Metromail surveys commissioned by Seventeen magazine, L'Oreal, Six Flags, Days Inns, R.J. Reynolds and Time-Life. The prison was paid $150,000 for the work.

Hal Parfait, the inmate serving seven years for breaking into a woman's house and raping her after threatening to kill her children, was transferred elsewhere after he wrote letters to at least two women whose identities and habits he had learned from the surveys.

But for about three months after his letter to Beverly Dennis came to light in 1994, the work continued pretty much the same way, records show. Then the Texas Legislature, responding to news accounts, barred sex offenders from record-entry work in prison. Overnight, Mr. Beckham lost 167 of his 430 inmate employees, and eventually 187 of them.

It was the same in the other Texas prisons, said John Benestante, director of state prison industries. "We lost some damn good programmers — pedophiles," he said. "Some of our best computer operatives were sex offenders."

But now Ms. Dennis was suing the Texas prison, and Mr. Benestante, a 6-foot-3 former air traffic controller, was deep in a review of all prison industry operations, especially those handling information for other public agencies, which pay by shifting public funds to the Department of Corrections.

Problems in the past had ranged from obscene "nasty-grams," inserted at random by prisoners stuffing envelopes for the Texas tourism department, to a ring accused of supplying car thieves with motor vehicle titles on commission. Well before the Dennis case, an inmate had used information on a motor vehicle title to contact a woman, and in a different department, an inmate managed to memorize a supervisor's Social Security number from a time sheet and ruin his credit rating.

Aside from the risks, he said, there were signs of shrinking demand, as more public agencies kept their records computerized from the start. But private companies were still eager to extract and compile valuable information from public records.

So Mr. Benestante had found a new high-tech information field with a promising commercial market, and had put the Ferguson prison, near Midway, Tex., ahead of the curve. Its former boot factory was a site for work in Geographic Information Systems, or G.I.S., a cutting-edge technology putting detailed maps and high resolution aerial photographs into computerized form.

How detailed? Plat records for Dallas show the location of the gas meter on each parcel. Aerial photographs of the city of Bryan, Texas, show the exact footprint of each house.

After the computer maps leave the prison, explained Robert Laake, the assistant administrator of the Ferguson "automated mapping-G.I.S." operation, "the Dallas planning and development department will place unique identifiers in each lot that will give them all the information they need — who lives there, what that block is worth."

The Ferguson prison has floor-to-ceiling

F. Carter Smith for The New York Times

At the Ferguson state prison near Midway, Tex., inmates use a cutting-edge technology to put detailed maps and aerial photographs into computerized form.

F. Carter Smith for The New York Times

At the Texas prison in Huntsville thousands of boxes of public records were processed before the business moved to another prison.

crash gates and tiers of two-man, 5-by-9-foot cells. The work site can be reached only by passing through a shower area lined with urinals, and walking across a yard where the men are routinely strip-searched on their way to and from the job. On the day of the visit, no inmates were at work because of a "lock-down" imposed after a rash of stabbings.

But inside the building, one could have been in any office. Supervisors demonstrated the simple computer tasks performed by the inmates, 120 men with an average sentence of 32 years. The price of their work was right. The unit was digitizing Van Zandt County's maps for $19,880, compared to a private sector bid of $60,000.

"If you don't send this here, the next stop is India," said Marilyn Beckham, the plant manager, referring to "information sweatshops" in Asia, Mexico and the Caribbean where much data entry is now done.

The strong privacy concerns raised about G.I.S. have little to do with using prisoners for the grunt work. This technology is proving an astonishingly powerful and lucrative commercial tool to crunch information from public records and private sector data banks and to spit out house-by-house information that can include everything from the tax assessment and the occupant's driver's license photograph, to details of consumer behavior collected by the likes of Metromail.

But Angela Pugh, a supervisor for the G.I.S. project at Ferguson, shrugged off the issue.

"Is the government going to sacrifice the money that can be made for a little bit of privacy?" Ms. Pugh asked.

A Business Technology

Using Compiled Data To Map Out Profiles

On an idyllic campus in Orono, Me., a professor who helped nurture the technology known as G.I.S. now wrestles with its dangers.

As Harlan Onsrud tells it, G.I.S. is a case study on the way new technology can change old stores of information into commercial gold and social dynamite. The story of its success, he said, underscores that both technological advances and sweeping business mergers have exploded old boundaries, leaving in the dust the sector-by-sector privacy legislation of the last three decades.

G.I.S. started as a way to map land, sea and sky across space and time. It has had enormously beneficial social uses, from pinpointing the origin of Legionnaire's disease to helping South Florida communities coordinate emergency relief after Hurricane Andrew.

But "there is no doubt that some uses, although currently legal, would be considered by most citizens in the U.S. to be highly intrusive and inappropriate," contended Mr. Onsrud, chairman of the University of Maine's department of Spatial Information Science and Engineering, part of the National Center for Geographic Information and Analysis.

In one G.I.S. application, businesses can feed car license numbers from a parking lot into a program and retrieve a customer's name, address, census tract information and demographic characterizations like "Hard-scrabble," "Sharecroppers," and "Furs and Station Wagons." Another program transforms a telephone number into a detailed profile of each prospective customer who calls an 800 number.

Public spaces are increasingly monitored electronically — for convenience, safety and traffic planning. But G.I.S. allows the results of this surveillance to be mapped with precision, identified by an individual's name or vehicle number without their knowledge, and correlated to a wealth of other information, including data culled from computerized public records of the kind the Texas prisoners have processed for 30 years.

Increasingly, cash-strapped government agencies are selling packaged public information to businesses or entering joint ventures to make the information more attractive to marketers.

Only a decade ago, when the Federal Bureau of Investigation sought clearance to enter all national databases, Congress said no.

"Now the commercial market has done it for them," Mr. Onsrud said. Government agencies like the F.B.I. "just have to pay like anybody else."

In the last three years or so, G.I.S. has spawned a booming "Geo Business" industry that applies its power to profile people and households for data-based marketing, health care, insurance, real estate and financial services. All three major credit bureaus and other giants in the information field have acquired or merged with G.I.S. mapping companies. They have forged new partnerships with big suppliers of data and data-mining software, and bought companies that deliver information to desktop computers on CD's or over the Internet. Their products include data bases that are continuously updated and parsed to yield an unprecedented level of detail on nearly everyone in the nation.

If information is like money, a company called the Acxiom Corporation is one of the merchant bankers of the age. Set in an industrial park in Conway, Ark., north of Little Rock, the corporate headquarters has a cathedral lobby with a facade of glass. But its heart is behind the locked doors of what a guide calls "the production war rooms," low-ceilinged bunkers where six robots inside small linked silos match data tapes at 60 miles an hour, while 20 mainframe computers swallow 1.3 billion bytes of data a second. G.I.S. is just part of the information infrastructure.

Acxiom's revenue grew by almost 50 percent in fiscal 1997, to $402 million. Its top customers include data kings like the AT&T Corporation, Wal-Mart Stores, Citibank, a unit of Citicorp, I.B.M., the Allstate Corporation and Automatic Data Processing Inc., which handles half the payrolls in America. The company now crunches all data for Trans Union. And last year R. R. Polk and Company, which says it collects and markets automotive and consumer information on 95 percent of the nation's households, used eight tractor-trailers to move its mother lode of data tapes from Michigan to a special warehouse in Conway.

This is a place where visitors are issued badges that turn purple if they leave the building — part of the aura of security Acxiom wants to convey to customers nervous about leaving their treasured customer data bases where their competitors also come to buy and barter for more data on their own customers, more names to "populate" computer models of their best prospects.

Many members of the information industry say technology is simply recreating the intimacy of small-town America in the days when the storekeeper knew all his customers by name, habit and history. But Mr. Onsrud, whose village in coastal Maine actually embodies that small-town ideal, flatly rejects the analogy.

"It's not an equal or mutual relationship,' he said. "We have information insiders and outsiders."

A Life and a Lawsuit

A Woman's Privacy Invaded By Industry

Beverly Dennis grew up in almost pre-industrial scarcity in a house her grandfather built himself. It had no electricity, no running water, and no indoor toilet to the day he died at 99. He never owned a car.

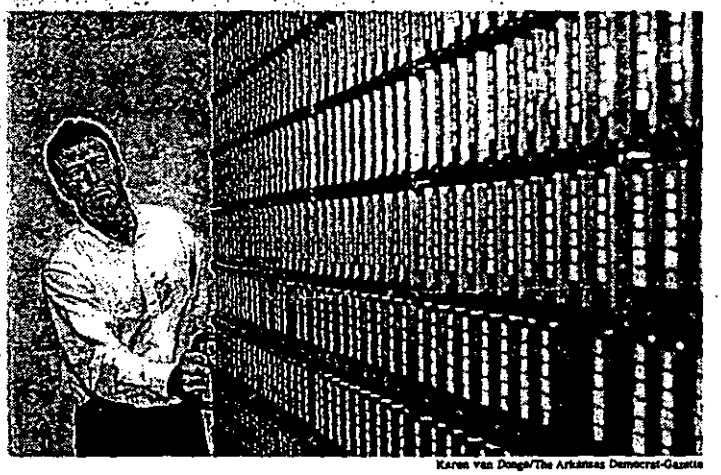
"I was raised very poor," Ms. Dennis said, sitting at the dining table in her carefully tended home. "My grandma used to boil her clothes on a stove, scrub on a washboard in the cold of winter. We didn't have much, but there was so much love."

Now Ms. Dennis has all the creature comforts of the industrial revolution, but she works standing at a noisy machine, stamping out 1,500 plastic bobbins an hour for less than $80 a day. "It's fast-paced work," said Ms. Dennis whose finger was recently mangled on the job. "I don't know how long I'll be able to do it."

For a few months several years ago, she had happily joined the brave new information economy at the Canton, Ohio, office of a national collection agency, G.E. Capital, owned by the General Electric Company. Computers automatically dialed telephone numbers from a disk, and each debtor's name, address, and payment history appeared on her computer screen. Ms. Dennis

Tony Dejak for The New York Times

Beverly Dennis, of Massillon, Ohio, filed a class-action suit against Metromail, a data-marketing company, after an inmate processing its information used it to harass her.



Karen van Dongo/The Arkansas Democrat-Gazette

Byron Mabry works for Acxiom, an information-processing company based in Conway, Ark., whose clients include AT&T, Allstate, I.B.M. and Wal-Mart Stores.

was monitored electronically as she followed a script demanding payment for everything from Apple Macintosh computers to children's shoes.

She failed to pass probation. "They told me I was too nice to be a collector," said Ms. Dennis, who raised two daughters on her own.

But this soft-spoken woman has a stubborn sense of justice, and it has carried her through tough times in a lawsuit that is trying to break new ground.

Last August, two of Metromail's lawyers questioned her for almost seven hours during a deposition in Austin, Tex. They wanted to know her Social Security number, her unlisted telephone number, when she had last dated and whether she drank. They probed into her health care and medication history, and had her name all her fellow employees. One of the Catch-22's of privacy litigation is its sacrifice of privacy.

Ms. Dennis, who earns less than $16,000 a year, said after she learned the identity of the inmate, she borrowed money to put in security lights, deadbolt locks, new windows and an alarm system in an unsuccessful effort to allay her pervasive sense of fear. Mr. Parfait, originally due to be released in 1995, is now to be freed next year.

"It's made me a different person," she said, describing sleepless nights, more frequent migraines and lost wages. "I can only tell you that I would give everything that I have if this would never have happened to me, because I am scared each and every day of everything, and I trust nobody after this."

Ms. Dennis said she wanted to warn other people so they would not make her mistake. But Shannon H. Ratliff, a lawyer for Metromail, suggested she had shown indifference to her privacy by giving her unlisted telephone number to Mark DeMarino, an investigative reporter at the Cleveland television station WJW-TV who helped her uncover the Metromail link, and by appearing with him on Geraldo Rivera's television show. The lawyer even asked why she had not sued the local station, since information from its reporter had upset her.

This was a line of attack rooted in the weaknesses of privacy case law, which has tended to see privacy as a "right to be left alone," in Justice Louis D. Brandeis's famous phrase — and to let that right collapse the moment personal information is surrendered for any reason.

But the critical issue today, privacy law experts agree, is usually not whether personal data should be collected and processed, but how data should and should not be used. Preserving privacy in this context is about the autonomy necessary to make decisions. That, too, has been recognized as a privacy interest by the Supreme Court — most notably in its decisions on abortion and contraception — but has not been developed much beyond decisions involving family and sex.

Privacy laws have been so narrow and spotty that the names of the movies rented at the video store where Ms. Dennis works on weekends are legally protected, but pay-per-view movies ordered at home are not. Medical and pharmacy records are not protected either and though the privacy of credit reports has been a matter of Federal law since 1970, a huge market in the information they contain has grown through its loopholes.

"The law of privacy has not kept up with the modern advances in technology, the modern rise of data transfer and information collection," Michael Lenett, Ms. Dennis's lawyer at the Cuneo Law Group in Washington, argued when the suit was filed last year. "This is the first case squarely to present the issue, who owns your personal and private information? Who controls it?"

But in April, when Mr. Lenett was still battling to get internal company documents, a judge in Travis County threw out the case's claim against the prison; an appeal is planned. The court ruled in part that misuse of information did not constitute misuse of property under the Texas Tort Claims Act, which makes the state immune from most damage suits.

"She's not complaining that somebody took a data-entry machine and whacked her on the head with it," explained Lin Hughes of Austin, Tex., a lawyer for Metromail.

The ruling leaves the claims against Metromail and its former parent, R. R. Donnelley & Sons: that the company unjustly enriched itself, and violated the privacy interests of the members of the class by fraudulently inducing them to provide personal information without disclosing how it would be processed and sold, and that it recklessly endangered their safety and inflicted emotional distress by negligently allowing felons to handle the information. The lawsuit seeks damages to be determined later and injunctive relief, including notification to all whose surveys went through the prison.

The company insisted in an unsuccessful motion to dismiss the case that it had no legal duty to tell consumers that the surveys would be processed by inmates. The facts consumers disclosed were not "highly intimate or embarrassing," the company argued, nor were they disclosed to the public at large.

Another cause of action recognized in Texas is conduct so "extreme and outrageous" that it is intolerable, and inflicts severe emotional distress. But, the company argued, "The mere receipt of a letter in the mail from an incarcerated inmate is not so extreme as to satisfy this standard."

Outside the courtroom, the company said its subcontractor was responsible for the prison work, and said that the job was stopped the same day Metromail learned of it. Internal documents tell a different story: Data tapes and surveys at the Texas prison were among the assets Metromail bought in 1993 when it acquired CMT, a marketing list company, and shipments and letters between the prison plant and Metromail continued until the work was finished, about three months after the letter came to light.

Documents gained through discovery also brought the four additional named plaintiffs to the case.

"I know the potential is out there to abuse people's information, but I really never gave it too much thought until I realized that my own information passed through the hands of a rapist or murderer," said one plaintiff, Patricia Mendiola, a part-time hospital lab technician in Wheaton, Ill., who is married to a systems analyst and has two children. "It made me so mad, the realization that all of this information ends up in a big data bank."

Robert DeSantis, who lives in Silicon Valley and was a civilian employee of two California military bases that closed, said that as a gay man, he worried about hate groups that could use such data bases to harass minorities.

Frenchie Holmes, a former fraud investigator for Pacific Bell in San Jose, Calif., who is now on disability, said she had been gullible. "You think they're going to send you products and trash that information, but they sell it. You fill out just one questionnaire and all of a sudden the whole world knows who you are."

Tim Fitzpatrick, a Metromail spokesman, said such sentiments were not common. "We certainly do not feel there's a class of people harmed as a result of this," he said. "Millions of people every year utilize direct marketing as a way to get things done. Millions of people are benefiting from it."

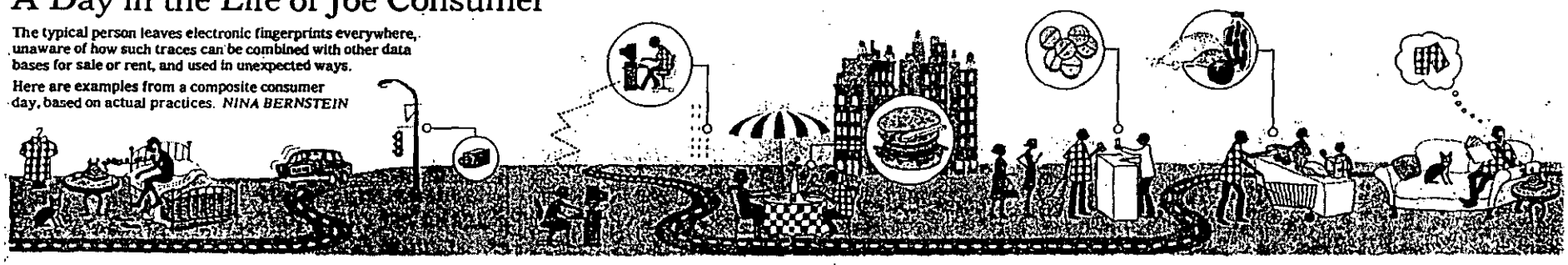
Indeed, Ms. Dennis counts herself as one of them. With two jobs, she shops by mail. "A new pair of curtains can make me so happy," she said. She does not know why the price should include her privacy.

"They are making millions of dollars off other people's lives who don't even know what they're doing," Ms. Dennis said. "They have turned my whole life upside down."

A Day in the Life of Joe Consumer

The typical person leaves electronic fingerprints everywhere, unaware of how such traces can be combined with other data bases for sale or rent, and used in unexpected ways.

Here are examples from a composite consumer day, based on actual practices. *NINA BERNSTEIN*



	Telephoning	Driving	Sending E-mail	Dining	Getting Prescriptions	Shopping	Mail Ordering
ACTIVITY	Joe calls an 800 number to check the pollen count.	Rushing to work, Joe inadvertently runs a red light.	At work, Joe criticizes his boss in E-mail to a friend.	Joe eats lunch at a restaurant that records each order on a computer.	Joe stops at the pharmacy to fill a tranquilizer prescription.	At the supermarket, Joe uses a discount shopper's card.	Before bed, Joe orders cufflinks and silk boxer shorts from a catalogue.
DATA CAPTURE	Joe's number is caught through Caller ID; his name and address are pulled from a public records data base.	Though the intersection is empty, a video camera captures his license number.	Joe's company reviews employee Internet activity and keeps copies of all E-mail.	Joe pays by credit card, linking his account number to his order of a bacon cheeseburger and fries.	His name, the drug and his doctor become part of the data base of the pharmacy chain.	The card links Joe's identity to every item he buys.	He pays by American Express, which adds his name to lists of "buyers of expensive jewelry."
FIRST USE	Joe is put on a list of allergy sufferers; it is sold to a drug company marketing allergy pills.	Joe is sent a traffic ticket in the mail.	After Joe's boss reads the E-mail, Joe is dismissed.	The restaurant checks his credit standing and sends him a discount offer.	The chain is part of a pharmaceutical company that combines the data with lists of magazine subscribers.	The supermarket chain uses a data-mining service to create profiles of its most profitable customers.	The catalogue company puts his name on a list of "male buyers of sexy lingerie" and trades it with other companies.
LATER USE	The list is linked with a profile of Joe and he is sent a coupon for the company's allergy medication.	Joe's insurance company finds the violation in a data base search and raises his rates.	Joe's unsuccessful lawsuit to regain his job shows up when a prospective employer uses an Internet investigation service.	The restaurant goes bankrupt and its list of men who are bacon cheeseburger lovers goes on the information market.	A rival tranquilizer company advertises in Joe's favorite magazine; company mailings urge Joe's doctor to switch.	Joe is deemed a prized customer and gets electronically-generated discounts; less loyal customers pay more.	Within two weeks Joe will receive four jewelry catalogues, five lingerie catalogues and a sex-videotape offer.

The New York Times; Illustration by Megan Jaegerman

PENDING PRIVACY BILLS

Bill No./ Date	Sponsor	# Co-Sponsors	Description
H.R. 52: 1/7/97	Rep Condit (D-CA)	1	Establishes a code of fair information practices for health information
H.R. 98: 1/7/97	Rep Vento (D-MN)	12	Prohibits an interactive computer service from disclosing to a third party any personally identifiable information provided by a subscriber without the subscriber's written consent
H.R. 537: 2/4/97	Rep Maloney (D-NY)	0	Amends Presidential Records Act of 1978 and the Privacy Act to ensure that FBI records containing sensitive information are protected for privacy and security.
H.R. 695: 2/12/97	Rep Goodlatte (R- VA)	165	Relaxes export control on encryption devices and creates new criminal penalties for using encryption to further a criminal act
H.R. 774: 2/13/97	Rep. Lofgren (D-CA)	27	Requires Internet service providers to offer filtering software; also amends Communications Act of 1934 to repeal provisions prohibiting using telecommunications device to make or initiate transmission of an obscene communication or depiction of sexual activities to a minor
H.R. 1180: 3/20/97	Rep. McDade (R-PA)	0	Requires Internet service providers to offer filtering software.
H.R. 1226: 4/15/97 (Sim to S 522 & 523)	Rep Archer (R-TX)	27	Criminalizes "browsing" of taxpayer files by IRS employees; on Senate Calender as of 4/17/97
H.R. 1287: 4/10/97	Rep Franks (R-NJ)	10	Prohibits computer services from disclosing a person's SSN without permission

PENDING PRIVACY BILLS

H.R. 1330: 4/15/97	Rep Kanjorski (D- PA)	18	Prohibits Federal officers and employees from providing access to Soc Sec Acct information, personal earnings and benefits estimate statement information, or tax return info through the Internet or without written consent of the individual, and to establish a commission to investigate the protection and privacy afforded to certain Gov't records
H.R 1331: 4/15/97	Rep Kennelly (D-CT)	0	Establishes a panel to assist the Commissioner of Soc Sec in developing appropriate mechanisms and safeguards to ensure confidentiality and integrity of personal SS records made accessible to the public
H.R. 1367: 4/17/97	Rep Barrett, T.	9	Prohibits Fed agencies from making available through the Internet certain confidential records, and providing for remedies in cases in which such records are made available through the Internet
H.R. 1972: 6/19/97	Rep Franks (R-NJ)	30	Prohibits "list brokers" from selling, purchasing info about children without written consent of parent; requires marketers to give access about child to parent, prohibits using prison inmate labor to process childrens' info; requires marketers to give lists to National Center for Missing and Exploited Children
S 144: 1/21/97	Sen Moynihan (D-NY)	1	Creates Commission to look at statistical agencies; it will look at privacy implications of collection and use of statistical information
S 376: 2/27/97	Sen Leahy (D-VT)	4	Relaxes export controls on cryptography. Creates new criminal penalties for using encryption to further a criminal act. Encourages key escrow infrastructure.
S 377: 2/27/97	Sen Burns (R-MT)	22	Relaxes export controls on cryptography. Creates Board to give law enforcement agencies special access to development of plans for privacy enhancing technology.
S. 504: 3/20/97	Sen Feinstein (D- CA).	2	Prohibits sale of personal information about children without their parents' consent

PENDING PRIVACY BILLS

S 665: 4/29/97	Sen Kerrey (D-NE)	1	Monitors the progress of the Telecommunications Act of 1996
S 771: 5/21/97	Sen Murkowski (R- AK)	1	Regulates the transmission of unsolicited commercial e-mail.
S 875: 6/11/97	Sen Torricelli (D- NJ)	0	Promotes online commerce and communications by regulating transmission of bulk unsolicited e-mail
S 909: 6/16/97	Sen McCain (R-AZ)	2	Facilitates national key escrow system; orders networks built with Gov't money to use key escrow. Maintains existing restrictions on export on encryption software.

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.

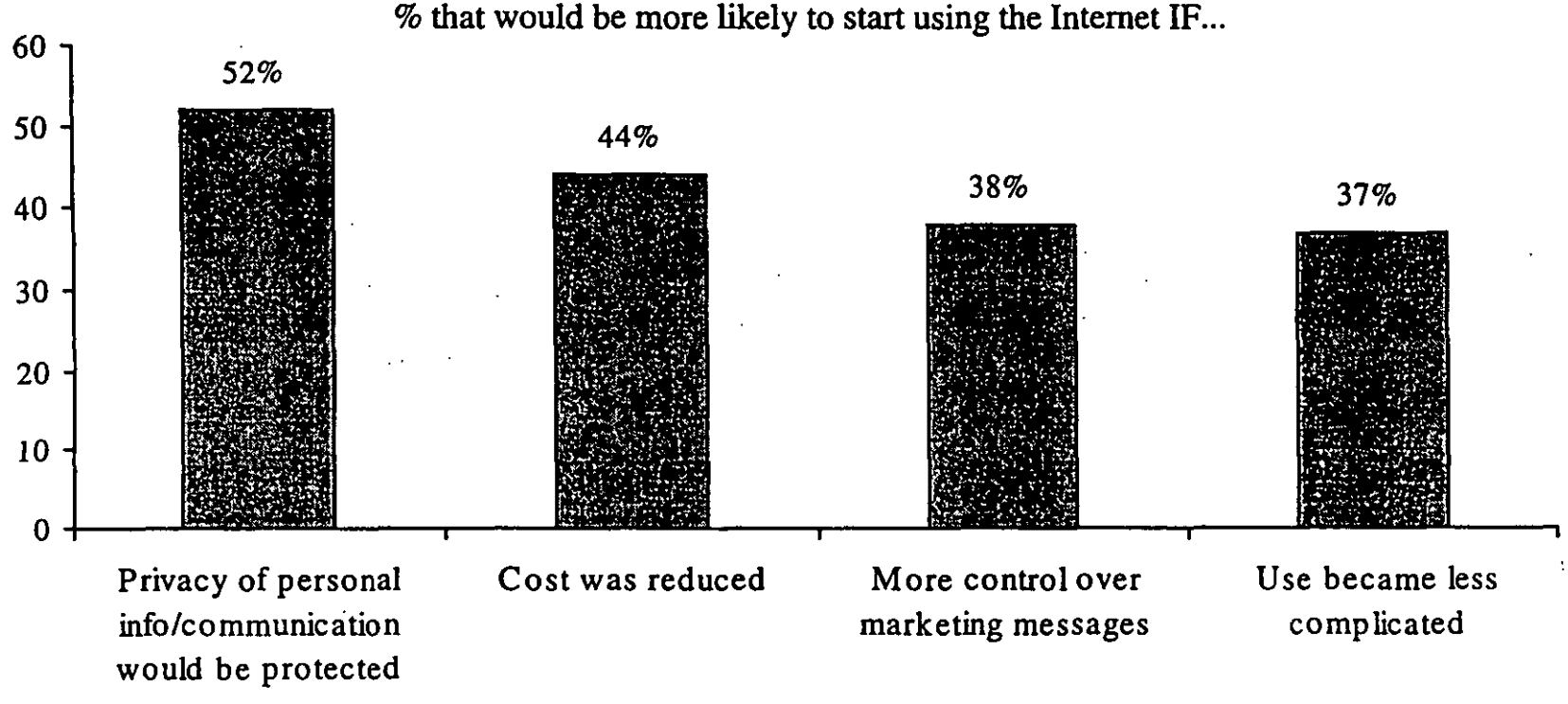
The low confidence that the survey results registered in the trustworthiness of online companies means that online business groups will have to engage in major educational programs to demonstrate that the policies and tools they support do provide an effective platform for reasonable online privacy.

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.**

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 c visitors to its sites, we shudder at th possibilities of what can be done wit this and similar electronic data cache DOD officials were very upset a coupl of years ago when the department dis covered one of the Internet browser com panies was surveying hard disks an sending information to a corporate data base. We suspect DOD's primary use fo the information is benign, or better stil noble in purpose: to garner informatio that might better serve the viewer. Bu do the benefits outweigh the risks?

While DOD may be the first agency t tackle the issue of Web logs and privacy, will certainly not be the last. We believ agencies would welcome some guidanc from the Office of Management and Buc get as they wrestle with crafting thei own policies.◀

FEDERAL Computer Week 7/7/97

File - consumer right to privacy

2. <u>Establish a Consumer Right to Privacy.</u> On October 27, 1992, the Clinton/Gore campaign released a document spelling out their vision of consumer protection. As an addendum to the Consumer Bill of Rights established by President Kennedy the campaign proposed there be "*The Right to Privacy To not have information provided by consumer for one purpose used for a separate purpose without the consumer's knowledge and consent.*" The Information and Technology Task force on Privacy, headed by OMB, has released its White Paper for comment and there is much activity, both public and private, currently in the area of privacy. The Administration would not short-circuit these discussions by adhering to this campaign promise.

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.