Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. fax cover sheet	[Personally Identifiable Information] [partial] (1 page)	10/25/1994	b(6)

COLLECTION:
Clinton Presidential Records
Staff Secretary
John Podesta (Subject Files)
OA/Box Number: 17336

FOLDER TITLE:
Privacy

2018-0662-S
rs3145

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. fax cover sheet	[Personally Identifiable Information] [partial] (1 page)	10/25/1994	b(6)

COLLECTION:
Clinton Presidential Records
Staff Secretary
John Podesta (Subject Files)
OA/Box Number: 17336

FOLDER TITLE:
Privacy

2018-0662-S
rs3145

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Nov 3

URGENT
ACTION
INFORMATION

EUROPEAN COMMISSION
WASHINGTON DELEGATION
Telecopier: (202) 429-1766
Telephone: (202) 862-9500

TELECOPY NO: 9447

COVER PAGE + PAGES

TO:Ms. Fran Wessel
Fax: 456-2215

DATE: October 25, 1994

FROM: Nicola Chausse NEC
CHRONO: TRADE/ 1125

ADDRESSEE PLEASE COPY TO:

SUBJECT: Meeting with Mr. Podesta and Mr. Mogg on Nov. 3.

As per our telephone conversation today please find the names of the EU members accompanying Mr. Mogg to the meeting :

Mr. John MOGG

Mr. Ian WILKINSON

Mrs. Anna SNOW

(b)(6)

Waved in

bio at back

+ Mike Nelson

done?

Andreas van Agt

Nov 3 NOV 3

Hold for meeting

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET

94 OCT 28 A11 : 31

Route Slip

==========

TO: JOHN PODESTA

___	**Take Necessary Action**
___	**Approval or Signature**
___	**Comment**
___	**Per Our Conversation**
___	**Let's Discuss**
XXX	**For Your Information**
___	**See Remarks Below**

FROM: Bruce McConnell Bruce **Date:** October 27, 1994
x53785

==========

REMARKS

Here are some notes, prepared by Maya Bernstein of my staff, for you to use in your meeting with Mr. John Moog, Director General in the European Commission, on November 3rd.

c: Sally Katzen
Maya Bernstein

Meeting with **Mr. John Mogg**
Director General in the European Commission
November 3, 1994
11:00am

Talking Points

1. Historically, in the US, the government has been seen as the dangerous user of information--the government in the 60s had lots of money, most of the big computers, volumes of information, and enforcement authority to use this information--great power. As a response to this situation and rising concern, the Privacy Act of 1974 regularized the maintenance and use of information by the Federal government.

2. Now, because of the explosion of information technology, the pendulum has swung somewhat in the other direction. The private sector in the US now rivals the government in the gathering, maintenance, and sharing of information about individuals.

[European model is generally the opposite -- they have traditionally regulated the private sector much more than the government.]

3. Polls here are showing that Americans are increasingly concerned about issues of privacy. In the private sector, we are seeing some of the "information intensive companies" such as financial and credit reporting companies, who have traditionally been the "bad guys," recognize that privacy is important to their customers. Companies are beginning to see that if they do not manage their data properly, some people will not want to do business with them. Some companies have established senior corporate policy officers to bring a privacy perspective to business decisions. Others have undertaken consumer education programs. We believe these are very positive steps.

4. We also recognize that the sharing of data across borders raises new international issues, so that while we protect privacy, we do not want to unduly restrict trade. The Administration takes these concerns seriously.

5. The last serious effort to look at privacy by the US government was in 1973 -- 20 years ago. [Report of the Secty of HEW's Advisory Committee on Automated Personal Data Systems" chaired by Willis Ware.] Since then, the environment has changed: electronic v. paper, distributed v. centralized, and private v. public sector threat.

6. The Clinton Administration is actively working on privacy. Our Privacy Working Group [of the Information Policy Committee (Sally Katzen chair), Information Infrastructure Task Force] has proposed a set of **Privacy Principles** which respond to the challenges of this new environment and lay out rights and responsibilities. An example: people should be able to find out easily how data about them will be used, and correct the data if it is wrong. Data collectors should not collect more information than they need, and they should tell individuals how their information will be used. Individuals must ask

why data is being collected, and verify it is correct. It uses an "opt out" model for consenting to use of information, rather than the "opt in" model more common in Europe. [Individuals may choose not to participate, but affirmative consent by an individual is not required.]

7. We're current reworking the principles based on public comments. [One criticism of the principles is that they do not address international issues particularly.] We intend for them to be used as a guide to incorporate into other laws. We intend to adapt them for the needs of particular sectors rather than establish them for the whole country at once.

8. The Administration has supported the idea of a privacy organization of some sort, most likely within the Federal government, that would focus attention on privacy -- have privacy as its portfolio. The Working Group is completing an analysis of the various roles such an organization might take -- advisory, advocacy, oversight, regulatory, technical assistance -- and is reviewing models of other countries. So far, none of the legislative proposals on creating such an organization would create regulatory powers nearly as great as the European privacy commissions. But there has been no decision yet as to what sort of organization we might create.

Suggested Points to Raise

What is the status of the Directive? When do you expect to get member state agreement to the Directive? When will the Directive go into effect?

For third country data transfers, who will decide what is "adequate protection" -- the Commission itself, member states, or both? How will the final determination be made?

We hope any process for determining adequacy of protection in third countries will be clear to us, and will allow for review.

Will contractual commitments to protect data be permitted to allow trans-border data flows? Do you envision model contracts coming into routine use to allow data flows to continue, in order to minimize trade disruptions?

Background on the EU Draft Directive on Protection of Personal Data
("Privacy Directive")

The EU Council of permanent Representatives was to discuss on October 31 the latest version of the draft directive. The commission and Germany (Eu Presidency) hope to hammer out remaining differences between member states quickly to reach a "common position" on the Directive in December at the European Council in Essen. At that point, it will go to the European Parliament, which will have 30 days to offer its opinion. The Directive could be issued in the spring.

From the US perspective, the major issue is trans-border data flow. The Directive would prohibit data flows to third countries (i.e. non-EU countries) which do not provide "adequate protection." (An EU-paid study of US privacy is likely to find a general failure to provide "adequate protection," although this will probably vary from sector to sector.) It is unclear who will make such a determination in any particular instance -- the Commission or each member state. The most recent version of the Directive allows transfer if the data will be adequately protected by appropriate contractual clauses. Depending on interpretation/implementation, the restrictions on third country transfers could potentially cause disruption in data flows and represnet a non-tariff barrier to trade.

Nov 3

URGENT
ACTION
INFORMATION

EUROPEAN COMMISSION
WASHINGTON DELEGATION
Telecopier: (202) 429-1766
Telephone: (202) 862-9500

TELECOPY NO: 8899 94 OCT 13 P12 : 02

COVER PAGE + PAGES

TO: Mr John Podesta
White House Staff Secretary
Fax: 456-2215
Attention: Fran

DATE: October 13, 1994

FROM: Anna Snow
CHRONO: TRADE/1059

Mr John Mogg, Director General in the European Commission, responsible, ia, for the Internal Market will be in Washington on November 2 and 3. He has overall responsibility for, ia. the issue of privacy and for this reason we would appreciate it if Mr Podesta could meet with Mr Mogg to exchange views on where the EU and the US are headed.

Mr Mogg is available as of 4 pm on November 2 and on November 3 in the morning. We would appreciate it if you could call Anna Snow at 862-9526 to set up an appointment.

11:00 a.m. Nov. 3

issues relating to NII

Andreas van Agt]

I asked for an update on issues from Bruce McConnell

✓ yes

no

John F. Mogg

John Mogg has held his present position of Director-General of DG XV (Internal Market and Financial Services Directorate General) in the European Commission since May 1993. Before that he was Deputy Director-General in the Internal Market and Industrial Affairs Directorate General from 1990. Between 1989 and 1990, he was Deputy Head of the European Secretariat in the United Kingdom Cabinet Office. Prior to that he held a number of senior positions with various United Kingdom Departments: these included Under Secretary in the Department of Trade and Industry and Principal Private Secretary to three Secretaries of State. From 1979 to 1982 he was the First Secretary at the United Kingdom Permanent Representation in Brussels. Mr Mogg's early career was spent in British industry with the Rediffusion group.

EQUIFAX
The Information Source

Melissa L. Bowen
Manager
Federal Government Relations

Equifax Inc.
Suite 800
1090 Vermont Avenue, N.W.
Washington, D.C. 20005
(202) 408-6893

EQUIFAX

Federal Government Relations
Suite 800
1090 Vermont Avenue, N.W.
Washington, D.C. 20005

94 FEB 22 A10:32

Dear Mr. Podesta:

Considering your involvement in information and privacy issues, I thought you might be interested in Mr. John Baker's testimony before the National Information Infrastructure (NII) working group. Please let me know if you need anything further.

Melissa Bowen

FW
file:
privacy

STATEMENT FOR THE PUBLIC MEETING

OF THE

INFORMATION POLICY COMMITTEE

WORKING GROUP ON PRIVACY

NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE

JOHN A. BAKER
SENIOR VICE PRESIDENT
EQUIFAX INC.

WASHINGTON, DC
JANUARY 27, 1994

IT IS A GREAT PLEASURE TO PARTICIPATE IN THIS PUBLIC MEETING OF THE INFORMATION POLICY COMMITTEE'S WORKING GROUP ON PRIVACY TO DISCUSS THE NEED FOR FAIR INFORMATION PRACTICES AS A MAJOR COMPONENT OF THE NATIONAL INFORMATION INFRASTRUCTURE. OVER THE PAST DECADE, AMERICANS HAVE WITNESSED DRAMATIC INCREASES IN THE SPEED AND EFFICIENCY OF COMMUNICATION SYSTEMS. SOURCES FOR MANY KINDS OF INFORMATION HAVE EXPANDED GREATLY, WITH COMPUTERIZATION AND TECHNOLOGY ENABLING MORE COMPREHENSIVE, CURRENT AND EASILY ACCESSIBLE DATA. WE APPEAR TO BE ON THE THRESHOLD OF EVEN MORE DRAMATIC CHANGE, AS EXPRESSED BY THE ADMINISTRATION'S VISION OF A NATIONAL INFORMATION INFRASTRUCTURE WITH THE POTENTIAL TO REVOLUTIONIZE OPPORTUNITIES FOR OUR CITIZENS, DEVELOP NEW TECHNOLOGIES, AND ENHANCE U.S. COMPETITIVENESS IN AN INCREASINGLY GLOBAL ECONOMY.

AS A COMPANY THAT, SINCE 1899, HAS PROVIDED INFORMATION SERVICES TO FACILITATE FINANCIAL TRANSACTIONS BETWEEN CONSUMERS AND BUSINESSES, EQUIFAX IS VERY ENCOURAGED BY AND SUPPORTIVE OF THE CLINTON ADMINISTRATION'S EFFORTS TO REVIEW PRIVACY ISSUES AND INFORMATION POLICIES TO ENSURE THAT FAIR PRACTICES ARE BUILT INTO THE INFORMATION INFRASTRUCTURE. WE BELIEVE IT IS CRITICALLY IMPORTANT THAT PROPER INFORMATION STANDARDS AND POLICIES BE

IDENTIFIED AS EARLY AS POSSIBLE - BASED UPON THE CORE VALUES AND SHARED BELIEFS OF OUR SOCIETY. THE TIME IS RIGHT FOR THE DEVELOPMENT OF A NATIONAL INFORMATION POLICY TO MAKE SURE THAT OUR PRIVACY OBJECTIVES ARE MET AND THAT OUR OVERALL GOALS FOR ECONOMIC GROWTH, COMPETITIVENESS AND CONSUMER PARTICIPATION ARE STRENGTHENED AND SUPPORTED BY RULES AND REGULATIONS THAT IMPACT VARIOUS INDUSTRIES AND SECTORS OF OUR ECONOMY.

ALTHOUGH THE 1974 PRIVACY ACT SETS A STATUTORY CODE OF FAIR INFORMATION PRACTICE FOR THE FEDERAL GOVERNMENT, THERE HAVE BEEN ONLY A FEW TRADITIONAL AREAS IN THE PRIVATE SECTOR WHERE STATUTES HAVE SET PRIVACY PROTECTIONS, SUCH AS CONSUMER REPORTING, DEBT COLLECTION, CREDIT BILLING AND CREDIT OPPORTUNITY. MORE RECENTLY, STATUTES HAVE ADDRESSED VIDEO RENTAL AND TELEMARKETING ISSUES, AND LEGISLATION IS NOW PENDING IN CONGRESS TO AMEND CONSUMER REPORTING REQUIREMENTS AND TO DEFINE RESTRICTIONS ON THE ACCESS TO MOTOR VEHICLE PUBLIC RECORD INFORMATION.

IT IS IMPORTANT THAT THESE AND OTHER LEGISLATIVE PROPOSALS AFFECTING CERTAIN TYPES OF RECORDS OR INDUSTRY SEGMENTS BE FOUNDED ON CONSISTENT PRINCIPLES OF INFORMATION USE AND PRIVACY. A CLEAR DEFINITION OF THOSE PRINCIPLES AND THE ESTABLISHMENT OF A

CONTINUOUS PROCESS TO ANALYZE AND RESOLVE INFORMATION POLICY ISSUES WOULD BE, IN OUR OPINION, A VERY POSITIVE STEP TO MAXIMIZE THE EFFECTIVENESS OF OUR INFORMATION INFRASTRUCTURE.

IT IS ALSO IMPORTANT THAT NEW LAWS AND REGULATIONS BE FLEXIBLE ENOUGH TO ACCOUNT FOR THE RAPID CHANGE LIKELY TO COME ABOUT WITH NEW TECHNOLOGY, SO THAT NEW INFORMATION SYSTEMS AND SERVICES ARE NOT INADVERTENTLY PREVENTED OR SMOTHERED. WE KNOW THAT NEW INFORMATION HIGHWAYS WILL ALLOW MUCH GREATER PUBLIC ACCESS TO A BROAD RANGE OF CHOICES AND WILL LIKELY ENABLE PERSONAL INTERACTION AND DATA INPUT TO INFORMATION SERVICES ON AN ON-LINE BASIS. NEW METHODS OF DATA TRANSFER AND NEW TECHNOLOGIES, SUCH AS CHIP CARD OR "SMART CARD" SYSTEMS, MAY RADICALLY TRANSFORM CURRENT INFORMATION FLOWS AND DECISION PROCESSES; SUCH SYSTEMS MAY PROVIDE ECONOMIC GAINS AND GIVE CONSUMERS MORE CONTROL OVER PERSONAL INFORMATION. WITH A NATIONAL CONSENSUS ON FAIR INFORMATION STANDARDS, WE WILL BE MORE LIKELY TO AVOID LEGISLATIVE RESTRICTIONS OR REQUIREMENTS THAT COULD FRUSTRATE SUCH NEW TECHNOLOGY AND INFORMATION MECHANISMS.

OUR EXPERIENCE AT EQUIFAX WITH PRIVACY ISSUES HAS FOCUSED

PRINCIPALLY ON THE REQUIREMENTS OF THE FEDERAL FAIR CREDIT REPORTING ACT, WHICH SETS STANDARDS FOR ACCURACY, PERMISSIBLE PURPOSES AND PROCEDURES FOR CONSUMER DISCLOSURE AND DISPUTE INVESTIGATION. WE HAVE ALSO LOOKED MORE BROADLY AT OUR INFORMATION POLICIES IN ORDER TO DEFINE FAIR USE PRINCIPLES CONSISTENT WITH PUBLIC OPINION AND EXPERT ADVICE.[1] WE KNOW THAT PERSONAL FINANCIAL INFORMATION IS SENSITIVE AND THAT PEOPLE INCREASINGLY VALUE THE ECONOMIC BENEFITS THAT DEPEND UPON INFORMATION, SUCH AS CREDIT, HOME OWNERSHIP, EMPLOYMENT AND INSURANCE. FOR THESE REASONS, WE BEGAN A SERIES OF INITIATIVES IN THE LATE 1980'S THAT HAS INVOLVED LEARNING MORE ABOUT PUBLIC ATTITUDES CONCERNING PRIVACY, STUDYING OUR OWN PRACTICES, IMPROVING OUR SERVICES TO CONSUMERS, AND USING TECHNOLOGY MORE EFFECTIVELY TO INCREASE DATA ACCURACY AND SECURITY. WE HAVE ALSO WORKED WITH OUR INDUSTRY THROUGH THE ASSOCIATION OF CREDIT BUREAUS TO ESTABLISH INDUSTRY-WIDE STANDARDS FOR ACCURACY, CONSUMER SERVICE AND PRIVACY.[2]

---

[1]APPENDED TO THIS STATEMENT IS OUR MOST RECENT PERSPECTIVE ON CONSUMER INFORMATION AND PRIVACY. A STATEMENT OF OUR PRIVACY PRINCIPLES IS ON PAGE 1 OF THE BROCHURE.

[2]THESE NEW STANDARDS ARE SET FORTH IN A PUBLICATION OF ASSOCIATED CREDIT BUREAUS ENTITLED "SETTING THE STANDARD: CONSUMER INITIATIVES IF THE CREDIT REPORTING INDUSTRY."

ONE OF OUR FIRST ACTIONS WAS TO ASK DR. ALAN WESTIN, PROFESSOR OF PUBLIC LAW AT COLUMBIA UNIVERSITY AND A LEADING EXPERT ON PRIVACY, TO CONDUCT PRIVACY AUDITS OF OUR BUSINESS OPERATIONS. THESE AUDITS HAVE BEEN ON-GOING FOR FOUR YEARS AND RECEIVE THE CONTINUOUS ATTENTION OF OUR SENIOR MANAGEMENT. IN 1990, WE SPONSORED A MAJOR SURVEY OF CONSUMER ATTITUDES ABOUT PRIVACY, CONDUCTED BY LOUIS HARRIS AND ASSOCIATES, WITH DR. WESTIN AS ACADEMIC ADVISOR. OUR SURVEY REPORT ENTITLED, "CONSUMERS IN THE INFORMATION AGE," OUR 1991 AND 1992 FOLLOW UP SURVEYS, AND OUR 1993 HEALTH INFORMATION PRIVACY SURVEY HAVE ALL REVEALED HIGH LEVELS OF PUBLIC CONCERN ABOUT THREATS TO PERSONAL PRIVACY.[3] PEOPLE HAVE EXPRESSED A GROWING DISTRUST OF GOVERNMENT INSTITUTIONS AND TECHNOLOGY, WITH THE MAJORITY OF THE PUBLIC EXPRESSING THE BELIEF THAT PROTECTION OF INFORMATION ABOUT CONSUMERS WILL GET WORSE BY THE YEAR 2000. AS RECENTLY AS MID 1993, 80% OF SURVEY RESPONDENTS SAID THAT CONSUMERS HAVE "LOST ALL CONTROL OVER HOW PERSONAL INFORMATION ABOUT THEM IS CIRCULATED AND USED BY COMPANIES."

---

[3]THE SURVEY COVERAGE AND TOPICS OF THESE FOUR STUDIES ARE BASED UPON ADVICE FROM A WIDE RANGE OF ORGANIZATIONS, GOVERNMENT DEPARTMENTS AND PRIVACY EXPERTS - INCLUDING THE U.S. OFFICE OF CONSUMER AFFAIRS. COPIES OF THESE SURVEY FINDINGS ARE AVAILABLE FROM EQUIFAX ON REQUEST.

AT THE SAME TIME, PEOPLE VALUE HIGHLY THE BENEFITS MADE POSSIBLE BY INFORMATION SYSTEMS. THE PUBLIC BELIEVES THAT COMPUTERS GIVE PEOPLE MORE CONVENIENT ACCESS TO USEFUL INFORMATION AND SERVICES, PROVIDE MORE INDIVIDUALIZED SERVICE THAN BEFORE AND IMPROVE THE QUALITY OF LIFE IN OUR SOCIETY. THE PUBLIC ALSO GIVES US HELPFUL INSIGHT AS TO HOW THESE POSITIVE AND NEGATIVE FEELINGS ABOUT PRIVACY THREATS AND INFORMATION BENEFITS CAN BE RECONCILED. TIME AND AGAIN, PEOPLE APPEAR TO EVALUATE THE PROPRIETY OF INFORMATION USE BY WEIGHING A NUMBER OF FACTORS, SUCH AS: THE LOGIC AND RELEVANCE OF THE PARTICULAR USE, THE DEGREE OF GENERAL KNOWLEDGE AND UNDERSTANDING ABOUT THE PRACTICE, THE POTENTIAL BENEFITS MADE POSSIBLE BY THE INFORMATION, THE SENSITIVITY OF THE UNDERLYING DATA AND THE INFORMATION STANDARDS EMPLOYED BY THE USERS. CONSUMERS APPEAR TO BE VERY WILLING TO DETERMINE FOR VARIOUS TYPES OF INFORMATION USE WHETHER OR NOT THE PRACTICES ARE FAIR.

THE CHALLENGE, IN OUR OPINION, IS TO SEARCH FOR THE CORE VALUES THAT UNDERLIE THESE PUBLIC NOTIONS OF FAIR USE. A GOOD STARTING POINT IS CERTAINLY THE INFORMATION STANDARDS SET FORTH IN THE 1974 PRIVACY ACT, ALONG WITH A REVIEW OF CONSUMER ATTITUDES EXPRESSED BY SURVEYS OF PUBLIC OPINION. WHILE THE EMERGING

NATIONAL INFORMATION INFRASTRUCTURE ADDS URGENCY TO THE SEARCH FOR A CONSENSUS ON INFORMATION POLICY, IT MAY BE THAT IT WILL NOT CHANGE THESE CORE VALUES. WE ARE REMINDED OF THE COMMENTS BY LAURENCE TRIBE IN 1991 AT THE FIRST CONFERENCE ON COMPUTERS, FREEDOM AND PRIVACY, ASSERTING THAT THE CORE VALUES EMBODIED IN OUR CONSTITUTIONAL PROTECTIONS SHOULD BE FULLY APPLICABLE "...WITHOUT REGARD TO THE TECHNOLOGICAL METHOD OR MEDIUM THROUGH WHICH INFORMATION CONTENT IS GENERATED, STORED, ALTERED, TRANSMITTED OR CONTROLLED." HE PROPOSED A 27TH AMENDMENT TO GUARD THESE VALUES FROM BEING ERODED OR "SENT TO OBLIVION" BY THE PROCESSES OF OUR NEW CYBERSPACE.

OUR NEW INFORMATION INFRASTRUCTURE, EVEN IF IT DOES NOT ALTER CORE PRIVACY PRINCIPLES, BUT ONLY INCREASES THE URGENCY TO IDENTIFY THEM, NONETHELESS WILL RAISE A NUMBER OF NEW FACT SITUATIONS AND DIFFICULT POLICY QUESTIONS HAVING MAJOR POLITICAL RAMIFICATIONS.

NEW INFORMATION SYSTEMS ARE INCREASINGLY NATIONAL, OR AT LEAST REGIONAL, IN SCOPE. IT IS CRITICAL THAT UNIFORM INFORMATION STANDARDS ASSURE SYSTEM EFFICIENCY AND COMPETITIVENESS, PUBLIC ACCESS AND CONSUMER PARTICIPATION. CONFLICTING FEDERAL RULES AND

STATE LAWS HAVE THE POTENTIAL TO BRING THE INFORMATION REVOLUTION TO ITS KNEES. AT EQUIFAX, WE HAVE ALREADY SEEN HOW DIFFICULT IT IS TO RESOLVE THIS PROBLEM OF FEDERAL AND STATE JURISDICTION IN A CONSUMER REPORTING CONTEXT. WHILE SURVEYS SHOW THAT THE PUBLIC PREFERS CONSISTENT AND COMPREHENSIVE FEDERAL PRIVACY STANDARDS,[4]THERE IS CONSIDERABLE RESISTANCE TO FEDERAL PRE-EMPTION BECAUSE OF VESTED POLITICAL AND ORGANIZATIONAL INTERESTS AND THE NOTION THAT STATES SHOULD BE FREE TO EXPERIMENT WITH ADDITIONAL REQUIREMENTS AND RESTRICTIONS.

AN NII PRINCIPLE IS THAT THERE SHOULD BE UNIVERSAL ACCESS TO INFORMATION RESOURCES AND THAT INDIVIDUAL PARTICIPATION IN THE INFORMATION ENVIRONMENT SHOULD BE MAXIMIZED. THESE OBJECTIVES WILL BE ACCOMPLISHED BY ON-LINE ACCESS AND NEW TECHNOLOGIES, AND THEY PRESUME THAT CONSUMERS WILL HAVE CERTAIN RESPONSIBILITIES, INCLUDING PAYMENT OF A FAIR PRICE FOR ACCESS AND SERVICE. ECONOMIC PENALTIES SHOULD NOT BE IMPOSED ON RECORD KEEPERS BY RULES REQUIRING THAT INFORMATION SERVICES BE FURNISHED FOR FREE OR BELOW COST. WHILE THERE MAY BE CIRCUMSTANCES JUSTIFYING A BELOW

---

[4][FOR EXAMPLE, THE MAJORITY OF THE RESPONDENTS IN THE 1993 HARRIS-EQUIFAX HEALTH INFORMATION PRIVACY SURVEY FAVORED FEDERAL LEGISLATION SPELLING OUT RULES FOR CONFIDENTIALITY OF INDIVIDUAL MEDICAL RECORDS RATHER THAN A PATCHWORK OF STATE LAWS AND ORGANIZATION INITIATIVES.]

COST OR FREE INFORMATION SERVICE, SUCH AS WHEN AN INDIVIDUAL HAS BEEN DENIED A BENEFIT BASED ON A CONSUMER REPORT, WHOLESALE REQUIREMENTS FOR "FREE" OR BELOW COST INFORMATION SERVICES WOULD ERODE NII AND STIFLE THE DEVELOPMENT OF NEW TECHNOLOGIES AND INFORMATION MECHANISMS.

AN IMPLICIT CONCEPT OF NII IS THE MAXIMIZATION OF INFORMATION RESOURCES TO ACHIEVE ECONOMIES IN THE USE OF DATA BASES AND HARDWARE AND SOFTWARE INVESTMENTS. THESE OBJECTIVES RAISE THE ISSUE OF ADDITIONAL OR SECONDARY USES OF COLLECTED DATA. EQUIFAX BELIEVES THAT PERSONAL INFORMATION SHOULD NOT BE USED FOR UNANTICIPATED PURPOSES WITHOUT NOTICE OR CONSENT APPROPRIATE TO THE CIRCUMSTANCES.[5] HOWEVER, POLICIES THAT MIGHT PREVENT ANY SECONDARY USE OF DATA SHOULD GIVE WAY TO A PROCESS THAT EXAMINES THE SENSITIVITY OF THE DATA, THE PURPOSES OF SECONDARY USE, CONSUMER EXPECTATIONS AND ECONOMIC BENEFITS IN ORDER TO DETERMINE THE PERMISSIBLE DEGREE OF ADDITIONAL USE AND ESTABLISH THE NOTICE OR CONSENT PARAMETERS.

ACCURACY, CURRENCY, RELIABILITY AND SECURITY OF DATA WILL BE

---

[5]SEE PAGE 1 OF OUR EQUIFAX PERSPECTIVES ON CONSUMER SERVICE AND PRIVACY.

PARAMOUNT REQUIREMENTS FOR A SUCCESSFUL NII. NEW TECHNOLOGY AND SOFTWARE ALGORITHMS CAN IMPROVE ACCURACY A GREAT DEAL, BUT FURTHER ENHANCEMENTS COULD BE ACHIEVED WITH BROADER USE OF PERSONAL IDENTIFIERS. IF THE PRIVACY CONCERNS CAN BE ADDRESSED BY RESTRICTING THE USE OF SUCH IDENTIFIERS FOR ACCURACY PURPOSES ONLY, PERHAPS AIDED BY NEW ENCRYPTION OR BLIND SIGNATURE TECHNIQUES,[6] THEN ACCURACY AND PRIVACY INTERESTS, PERHAPS, CAN BE RECONCILED - WITH GREAT BENEFITS FOR THE NII. WE RECOMMEND THAT THE WORKING GROUP EXAMINE THESE TECHNOLOGIES TO EVALUATE THEIR PRIVACY FEATURES AND THE PRACTICALITY OF THEIR APPLICATION.

ON THE ASPECT OF SECURITY, IT MIGHT BE OF VALUE TO LEARN THE EXPERIENCES OF VARIOUS LAW ENFORCEMENT EFFORTS AND ANY GAPS IN APPLICABLE LAW THAT COULD BE CLOSED TO ACCOMPLISH SWIFTER AND MORE EFFECTIVE PROSECUTION OF THOSE WHO BREACH CONFIDENTIALITY OR BREAK INTO INFORMATION SYSTEMS. INDIVIDUALS WHOSE PERSONAL DATA HAVE BEEN IMPROPERLY ACCESSED, ALTERED OR USED SHOULD HAVE QUICK AND MEANINGFUL REMEDIES AGAINST DATA CRIMINALS.

---

[6]DAVID CHAUM'S ARTICLE IN SCIENTIFIC AMERICAN, AUGUST 1992, ENTITLED, "ACHIEVING ELECTRONIC PRIVACY", DISCUSSES A THEORETICAL IDENTIFICATION SYSTEM USING BLINDED DIGITAL PSEUDONYMS TO IMPROVE PRIVACY AND SECURITY.

THE NII ENVISIONS AN ATMOSPHERE IN WHICH CONSUMERS HAVE ACTIVE RELATIONSHIPS WITH INFORMATION SYSTEMS. EFFECTIVE INTERACTIONS WILL LIKELY REQUIRE DATA PROVIDERS TO ADOPT TRUSTEE OR STEWARDSHIP ATTITUDES IN THEIR USES OF INFORMATION. WHATEVER CAN BE DONE TO ENCOURAGE SUCH ATTITUDES BY A PARTNERSHIP EFFORT BETWEEN GOVERNMENT, BUSINESS AND CONSUMERS WOULD BE A VERY POSITIVE DEVELOPMENT.

UNDER A PARTNERSHIP APPROACH, CONSUMERS WOULD HAVE INCREASED CONFIDENCE BECAUSE OF AN AGREED UPON STANDARD OF FAIR INFORMATION PRACTICES; GOVERNMENT WOULD HAVE A CONTINUING PRIVACY OVERSIGHT AND SET THE CLIMATE FOR INVESTMENT AND COMPETITION; AND THE PRIVATE SECTOR WOULD HAVE INCENTIVES TO BUILD NEW SYSTEMS AND TECHNOLOGIES BECAUSE THE BENEFITS OF NEW INFORMATION SERVICES WOULD BE RECOGNIZED WITHIN AN OVERARCHING, NATIONAL INFORMATION POLICY.

THIS APPROACH COULD MEAN BOTH SELF REGULATION AND SHARED REGULATION, EMPHASIZING COOPERATION AND CREATIVITY. FOR SEVERAL DECADES, THE FTC HELD REGULAR "INDUSTRY COUNCILS" THAT BROUGHT GOVERNMENT AND INDUSTRY TOGETHER IN A COOPERATIVE EFFORT TO IDENTIFY PROBLEM ISSUES, DEVISE SOLUTIONS AND MONITOR PROGRESS.

RECENTLY, CONGRESSMAN ED MARKEY INTRODUCED A TELECOMMUNICATIONS PRIVACY BILL CALLING FOR THE FCC TO HOLD HEARINGS AND PROMPT THE DEVELOPMENT OF PRIVACY CODES FOR VARIOUS TELECOMMUNICATIONS SERVICES.

THE FEDERAL GOVERNMENT CAN AND SHOULD BE ACTIVE IN PROMOTING PRIVACY AND DOING MANY OF THE THINGS THAT MIGHT BE CONDUCTED BY A PRIVACY PROTECTION COMMISSION UNDER SENATOR SIMON'S RECENTLY INTRODUCED PRIVACY PROTECTION ACT OR A DATA PROTECTION BOARD UNDER PROPOSALS BY CONGRESSMAN WISE IN THE PREVIOUS CONGRESS. COORDINATION OF PRIVACY POLICY, RESEARCH OF CONSUMER ATTITUDES, PUBLIC EDUCATION ABOUT PRIVACY ISSUES, HEARINGS, ADVISORY ACTIVITIES, AND INTERACTION WITH PRIVACY COMMISSIONS OF OTHER COUNTRIES - ARE ALL FUNCTIONS THAT WOULD BE POSITIVE AND HELPFUL TO OUR INFORMATION INFRASTRUCTURE IF CARRIED OUT IN THE SPIRIT OF COOPERATION AND PARTNERSHIP THAT HAS MARKED THE ADMINISTRATION'S WORK ON NII AND THE OBJECTIVES OF ITS TASK FORCE, INFORMATION POLICY AND PRIVACY WORKING GROUP EFFORTS.

WE ARE ENCOURAGED BY THESE REVIEW PROCESSES TO HELP ESTABLISH A NATIONAL INFORMATION POLICY GROUNDED ON THE SHARED VALUES OF OUR CITIZENS. WITH THE INCREASED PUBLIC CONFIDENCE THAT

SUCH A POLICY WILL GENERATE, NII WILL TAKE A MAJOR STEP TOWARD THE OBJECTIVE OF AN OPEN MARKET OF IDEAS AND COMMERCE FOR THE BENEFIT OF ALL AMERICANS. THANK YOU FOR THE OPPORTUNITY TO PRESENT THESE COMMENTS AT THIS PUBLIC MEETING, AND WE LOOK FORWARD TO ASSISTING THE WORKING GROUP'S EFFORTS IN ANY WAY POSSIBLE AS IT MOVES FORWARD WITH FURTHER STUDY AND RECOMMENDATIONS.

Consumer Information and Privacy

The Equifax Perspective

EQUIFAX

Equifax believes that individuals should have the following rights:

The right to be considered for credit, insurance, employment and other benefits on their own merits, based on their record of actions and performances.

The right to be treated with respect and fairness whenever information about them is used.

The right to privacy consistent with the requests and demands they make of business.

The right to have their applications for benefits or opportunities evaluated on the basis of relevant and accurate information.

The right to know what information has been provided about them for consumer reporting purposes.

The right to know what consumer data is being maintained about them and to be able to review the information in a reasonable time, at a charge that is not excessive, in a format that is understandable, and with an ability to challenge and correct inaccurate information.

The right to expect that information about them that is collected or stored for consumer reporting purposes will not be used for unanticipated purposes without notice or consent appropriate to the circumstances.

The right to expect levels of accuracy consistent with sound practices of record keeping and information systems management.

The right to have information about them safeguarded through secure storage, confidential handling within the organization, and careful transmittal to authorized and legitimate users.

The Role of Equifax: Information Stewardship

What does Equifax do?

Equifax helps people and businesses complete financial transactions.

Each year millions of people use credit cards, write checks, open charge accounts, apply for jobs, and insure their lives, health, homes and property. All these transactions require timely and reliable personal information. Equifax gathers such information, processes it, and transmits it to the banks, retailers, insurers, and other organizations that use it as the basis for granting these benefits.

What information do we gather?

The information that Equifax gathers must be relevant to the intended transaction and helpful to the decision-making process. In determining what information to report, Equifax draws upon custom, changing social values, and the needs of the marketplace. Equifax gathers and reports information that consumers and businesses recognize as necessary for the conduct of business.

For example, for a lender to approve a loan transaction, we provide information on a consumer's credit accounts, including the dates opened, dates of last activity, terms agreed to, balances, current status of accounts, and payment history.

For property or automobile insurance transactions, we provide information on the claims filed, including type of claims, identification of the policyholders, types of policies and insurance companies, status of claims, and amounts paid, where applicable.

Equifax does not gather or store information that has no bearing on the benefits for which a consumer is being considered. Consumers have the right to review the information, to ask questions, and to challenge and correct inaccurate consumer report information.

What do we do with this information?

Some information is gathered and stored on databases for retrieval when a financial transaction takes place. Often, we store and maintain information that is historical in nature and used repeatedly over time, such as a credit history. The best method of determining credit worthiness, for

example, is to know how a person has managed financial obligations in the past. In other cases, we may gather information on a one-time basis without retention to help a business make one specific determination — such as whether to employ an applicant or underwrite an automobile insurance policy.

How does Equifax benefit consumers, business and the economy?

Each day American consumers buy thousands of homes, cars, and major appliances. Most of these transactions are made on credit. The availability and reliability of credit history information makes it possible for these transactions to occur rapidly and efficiently.

Insurance premiums are more reasonable in cost because underwriters can obtain the necessary information to evaluate a person's application on his or her own merit. For example, life and health insurance underwriters, with a direct authorization by the consumer, can obtain from the consumer's attending physician a statement providing relevant information about the applicant's current and historical medical condition. Such medical information is not databased by Equifax.

Underwriters can also request Life & Health Underwriting Reports, which provide information needed to validate statements made on the insurance application. For the property and casualty insurance markets, Equifax offers an automated claims exchange database on automobile and property claims to help insurance companies evaluate the costs and risks of insuring drivers and motor vehicles. Information services also help reduce the costs of exaggerated or fraudulent claims.

Employers who use Equifax Employment Reports are better able to evaluate prospective candidates for particular job positions. These reports help confirm statements made by applicants and help employers protect the safety of employees, customers, and the public. They also help protect employers against substantial legal liability for negligent hiring.

Who can order or obtain consumer information?

First of all, the consumer, the subject of a report, has the right to know the contents of a report provided about him or her. Whether for credit, insurance, or employment, information gathered or reported by Equifax is available to the individual consumer. If a consumer questions any information in the report, we will recheck the information and make any corrections if there is erroneous or out-of-date information. If we can no longer confirm any particular information, we will remove it from the report. If we do confirm it, we will include the consumer's written statement about the information in question.

What legal requirements and voluntary practices govern our business?

The federal Fair Credit Reporting Act (FCRA) and various state laws govern the conduct of our business. Users of our services must comply with this legislation, which specifies punishment and fines for improper and illegal accessing of consumer report information. Federal and state laws do provide a basic framework for our information practices, but, in many instances, Equifax goes beyond the legal requirements to set additional standards and procedures in the interest of consumer service and privacy. For example, though not required by law, our practice is to provide consumers who have not been denied credit, insurance, or employment with detailed disclosure of all information in our file in easy-to-understand formats and with a system of toll-free access. Our information consultants are trained to provide quick and courteous service, and, whenever a recheck of information is requested, we follow up the process with a new, complete report.

We are permitted to furnish consumer reports only to those businesses having a permissible purpose — credit evaluation, insurance underwriting, employment decisions, the granting of a license, or other business needs involving a transaction with the consumer. To ensure that consumer report information is kept strictly confidential and is used only for permissible purposes, we carefully screen applications from businesses who want to receive consumer reports. We visit each applicant's premises to confirm identity and purpose of use, and we require every user to certify that reports will be requested in compliance with the aforementioned legal requirements.

New Realities of Consumer Information Services

INFORMATION FOR CONSUMER TRANSACTIONS has evolved from personal relationships between merchants and consumers in a local setting to a current global situation where financial transactions are between strangers, often located in different parts of the country or the world. As technology speeds up processes, consumers now expect loans and check approvals in minutes or seconds, rather than the several days or weeks that once were required.

In the past, consumer information services have provided information about consumers for business. Often consumers have not been active participants in the information process. Today, that is changing. Through several years of research and dialogue, we have recognized the growing importance of information to the individual and the importance of treating individuals as valued stakeholders in the consumer reporting process.

Information about consumers is also for consumers. Equifax wants to give people easy access to information reported about them and to foster understanding of the three-way consumer reporting process among the consumer, benefit granter, and Equifax, the reporting agency. Our goal is to deliver high quality, personal service to individuals on whom we maintain information and to provide that service in a manner that goes well beyond the letter of the laws which guide the information industry.

The New Emphasis on Individual Rights

OUR CONSUMER SERVICE GOALS have been based in large part on our continuing sponsorship of public opinion surveys conducted by Louis Harris and Associates with Dr. Alan Westin of Columbia University as academic advisor. Our 1990 landmark survey, The Equifax Report on Consumers in the Information Age, and annual follow-up surveys have revealed that most Americans are concerned about threats to their personal privacy and desire a larger degree of participation in the ways that information is gathered about them and used. The survey also found that Americans are basically pragmatic about the use of their personal financial information, value the benefits made possible by the collection and use of that information, and will support such uses as long as they know fair information practices are observed.

In a new age of technology and expanding information sources, there is clearly a need for a continuing balance between the legitimate information needs of our economic system and the privacy interests of our citizens. Current consumer protection law provides a good framework for maintaining the appropriate balance, setting out permissible purposes, establishing accuracy standards, and allowing consumers to view data and seek explanations or corrections, if necessary.

As the leading provider of information for consumer financial transactions, Equifax continues to be a pioneer in consumer-oriented initiatives, expecially in the area of consumer privacy. We believe the information we gather and provide is the lubricant on which our nation's economy runs and prospers. We also believe in the rights of individuals to participate in decisions over the use of information about them: to know what information is gathered, what is done with it, who can obtain it, and what benefits accrue as a result of its proper availability.

Putting Equifax Beliefs Into Practice

THE FOLLOWING ACTIONS and initiatives have been undertaken to enhance privacy protection, improve information accuracy, and provide professional service to consumers.

- We conduct annual national surveys of consumer attitudes about privacy and fair information use.
- We consult with privacy experts, representatives of consumer groups and commentators about privacy concerns and data protection issues.
- We conduct regular privacy audits of our various information services. Dr. Alan Westin, Columbia University Professor of Public Law and Government and noted privacy expert, conducts these audits.
- Security systems are continually reviewed and strengthened to protect information systems.
- New state-of-the-art software logic helps ensure maximum accuracy in data input and delivery.
- Expert systems help ensure data integrity; automated systems track the progress of consumer requests for reinvestigation.
- Standardized formats and data reporting procedures improve speed and consistency of data.
- The Equifax Office of Consumer Affairs assures quality service and acts as an ombudsman for consumers.
- Equifax opened a first-of-its-kind Information Service Center in December 1991 - with excellent service standards and a service attitude that treats consumers as valued customers.
- Information consultants provide courteous and prompt disclosure and reinvestigation of questions or disputes. Automated systems deliver rapid service.
- Redesigned report formats improve consumer understanding of information.
- Periodic surveys of consumers who have obtained their credit report help us track performance and assure continued high service quality.

What's Next For Equifax?

WE ARE PLEASED with the progress that has been made, but we know there is more to be done. We continue to review our procedures and to look for ways to make our information more meaningful and our service more effective to businesses and consumers.

We know that continuing changes in technology, information use and public opinion must be monitored very closely and that we must adjust our practices whenever possible to improve information quality, accuracy, consumer service and privacy.

Our intent is to be the preferred steward of consumer information. We at Equifax pledge to conduct our business in accordance with the beliefs expressed in this document. We are committed to superior information practices worthy of the public trust.

What if I Have a Question?

PLEASE WRITE OR CALL us if you have any questions about your rights or our information practices. We will answer your inquiries or direct you to our appropriate business activity in accordance with your request.

Equifax Inc.

Corporate Public Affairs

1600 Peachtree Street, N.W.

Atlanta, Georgia 30309

(404) 885-8231

file privacy

or confiscate property--in other words, citizens are guaranteed a chance to set the record straight.

When Lou Harris, in 1990, asked Americans to agree or disagree with the statement, "If we rewrote the Declaration of Independence today, we would probably add privacy to the list of 'life, liberty and the pursuit of happiness' as a fundamental right," by an overwhelming 79% - 19% margin, Americans agreed.

In today's environment, both the public sector and the private sector have embraced information technology as the only way to manage the huge stores of data they need to run their programs and enterprises. With the widespread use of information systems, the gathering of a wide variety of information is simple, quick and relatively inexpensive. So is the ability to collect, access, modify, revise, repackage and resell information products. Today's information privacy laws, practices and policies, however, offer only a patchwork approach to protecting privacy in this new environment.

Innumerable data bases exist. Some, held by government entities are readily available to anyone who wishes to see them. These might include records on real estate ownership, court cases, tax liens, bankruptcy filings, voter registration, auto ownership, driver histories, and marriage licenses. In addition, the private sector holds and controls access to many sensitive records, which are relatively free of regulation. These include financial, medical, employment, and telephone records. Much of this kind of information, whether originating in the public or private sector, can be sold and resold by the original gatherer, private investigator or information brokers without the record subjects' consent or knowledge.

There are also the databases held by organizations operating under privacy laws. These records, though protected, are accessed legally when authorized by a body that deems it in the interest of society to do so, for example for law enforcement purposes, health care research or better management to save taxpayer dollars. They are also unfortunately illegally accessed by employees, computer hackers and others.

The bright side of the use of information technologies is that individuals benefit when data is used in their interest. They receive better information, better service and decisions about them are made in a productive or informed way. They may be singled out for their accomplishment and for who they are or for what they have done and rewarded for it in various ways. And society, in general, can benefit by legitimate uses of records. We know the demographics, needs and desires of various constituencies, we discover problem areas and can provide better service, often at lower cost.

Moreover, while media reports often focus on the use of modern information technology to invade privacy, the advances in

National Performance Review Recommendations

The NPR made specific recommendations on protecting privacy and confidentiality of records. Specifically, the task group looking at these issues recommended that the President establish a Privacy Protection Task Force that would establish uniform privacy protection practices and acceptable implementation methods for these practices. The Task Force would also propose legislation creating a permanent national Data Protection Board.

The Information Infrastructure Task Force (IITF) NII

The IITF, like the NPR, operated under the aegis of the Vice President. Whereas the NPR focus is primarily on improving government performance, the IITF has a broader nationwide mandate. It grows from the vision of the United States as "a seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at users' fingertips. Development of the National Information Infrastructure (NII) will change forever the way people live, work, and interact with each other." (from the National Information Infrastructure: Agenda for Action.)

This effort is being chaired by Ron Brown, Secretary of Commerce and has three committees:

- The Telecommunications Policy Committee
- The IITF Applications Committee, and
- The Information Policy Committee

The Information Policy Committee is chaired by Sally Katzen, Administrator of the Office of Information and Regulatory Affairs. Under this Committee is a subcommittee that has a privacy mandate. PAT FALEY This group has developed a workplan to investigate what policies are needed to ensure individual privacy in the NII, while recognizing legitimate societal needs for data, including those of law enforcement. The group is currently meeting with privacy experts to gather data as widely as possible. It intends to hold a public hearing later this year or early next. It will next develop proposed polices for ensuring privacy in the NII. It is also within the charter of the group to develop privacy legislative proposals. We think that this group will carry out the intent of the NPR recommendations. Although the IITF privacy group will look much more broadly at privacy issues.

Medical Records Privacy

The Department of Health and Human Services has convened a task force on the privacy of medical records. Its report will be coming out soon. In addition, the administration's health care reform proposal will have a privacy component.

Tom Silva 6406

The Health Security Plan

PRIVACY AND SECURITY OF HEALTH CARE INFORMATION

Personal medical information poses a critical dilemma for health care reform: accurate, timely data is critical to delivering the highest quality and most efficient care and yet information about a person's medical history is among the most sensitive information our society maintains.

In today's health care system, no comprehensive privacy standards for health care information exist. There are no legal protections to guard against the inappropriate or malicious disclosure of personal medical information. The result has been an increasing number of privacy lawsuits and a growing sense of distrust among the public.

The Health Security plan will contain aggressive measures to protect personal medical information and rebuild trust between patients and health care institutions and providers. Iron-clad privacy protection -- including national standards on accountability, information protection and enforcement -- will be a critical element of the plan. These standards shall be based on core principles established by the legislation, such as the following:

- *Any disclosures permitted by law shall be of the minimum amount of information necessary to achieve the lawful purpose of that disclosure.*

Principles to Maintain Patient Rights and Board Responsibility

- Every patient shall have the right to know in what locations any individually identifiable information is maintained and the purposes for which such information could be disclosed.

- Every patient shall have a right of access to individually identifiable information in order to see, copy or correct such records.

- The plan directs the National Health Board to promulgate standards to protect the privacy of individually identifiable information which is collected and/or reported as part of the new system.

- The Board will be directed to prepare for the President and for Congress a detailed proposal for comprehensive medical records legislation.

Health Data and Health Identification Numbers Protected from Other Uses

- The Health Security plan prohibits any use of the security card except for the purposes of obtaining the items and services in the guaranteed national benefit package.

- Anyone who requires the display or use of the card, or who requires the disclosure or use of the identifier number, for any other purpose will be subject to criminal penalties.

- Data collected as part of the operation of the new health care system will be used only for that purpose and not shared with any other entity.

- Neither regional nor corporate alliances will be allowed to use health care information as a basis for employment decisions.

- The national privacy policy will explicitly forbid linking of health care and non-health care information through health identification numbers.

States Can Continue Anonymous Testing for Diseases

- States whose health policies allow anonymous testing for specific diseases, such as AIDS, may continue that policy.

October 8, 1993

Major Policy Issues/Questions

- What records should be governed by principles of health record privacy?
- Should "specially sensitive" records receive special treatment?
- What is the impact of automation on the privacy of health records?
- What concerns are raised by use of a unique identifier for health records?
- At what level should legislation be enacted to protect health information?
- What constitutes informed consent for disclosure of health information and under what circumstances may informed consent not be a sufficient basis of disclosure?

Major Policy Issues/Questions (cont.)

- Under what circumstances should record keepers be allowed to disclose records? How will policies and requirements be enforced?
- What type of structure is needed to oversee privacy policy, confidentiality and security matters and violations?
- What training, education and awareness programs should there be both for individuals regarding there own records and for those working with health records?

Health Record Systems of the Future

- A comprehensive **longitudinal computer-based patient record** (clinical, financial and research data, including diagnostic images or pictures)
- A "national" **electronic network** for accessing this health record for a variety of purposes (primary care, insurance payment, peer review, cost containment, public health and research purposes)
- Use of a **smart card** for purposes ranging from providing health insurance coverage information to providing a conception-to-death record of all health care
- Use of **unique patient-specific identifiers**

Draft
Subject
to Change

Work Plan
Working Group on Privacy
Information Policy Committee
Information Infrastructure Task Force (IITF)

September 10, 1993

PROBLEM:
We are moving rapidly from a paper-based world into one dominated by electronic information technologies. To ensure the existence of individual privacy protection, existing laws, practices and policies must be examined and adapted to the new environment.

BACKGROUND:
In 1972, the National Academy of Sciences reported that,

> "It is technologically possible today, especially with the recent advances in mass storage memories, to build a computerized, on-line file containing the compacted equivalent of 20 pages of typed information about the personal history of selected activities of every man, woman, and child in the United States, arranging the system so that any single record could be retrieved in about 30 seconds."

Congressional response to this possibility and perceived privacy abuses by the government was to ask "the fundamental question about the rights of the individual citizen in our society: is it in our best interest to allow the government to continue to expand its files on citizens and to gather detailed information on any citizen without proper safeguards for the privacy of those individuals?"

The answer for that time was passage of the Privacy Act of 1974, which attempted to put in place for the Federal government a statutory Code of Fair Information Practices. For the private sector, however, few statutory solutions were found, and then only in those areas where egregious acts were seen to have taken place, e.g. credit reporting.

But the world of that time was a world where information was managed on paper. The main storage device was a file cabinet. Information was transmitted through the mail. We are in a different world now. One where computers manage our information and the possibilities for both invading and protecting privacy are greatly magnified.

While personal privacy was not specifically guaranteed in the Constitution, courts have found that various privacy principles are found in it. It restricts the means that government may employ to gather information about its citizens, and the uses which government can make of such information. It prevents the government from intruding into citizens' lives through unreasonable searches and seizures. And it requires that citizens be given "due process of law" before the government can impose punishment, fines,

~~As a starting point, the task force agreed that~~ traditional privacy principles, embodied in the Constitution, must guide public policy with respect to communications privacy and the new technologies. Few social and commercial relationships remain unaffected by the introduction of new technologies such as cellular and cordless phones, electronic mail, bulletin boards, and pagers. Traditional barriers of distance, time, and location are disappearing as our society comes to take these advanced forms of communication for granted. As new technologies become available, a tension is often created between existing societal values and expectations, and the commercial opportunities and outlets for personal expression created by these advances.

~~The task force agreed that~~ peoples' expectations of privacy should not be measured against what is technically possible. People care deeply about their privacy, and cherish the ability to control personal information. Even if they have done nothing wrong, or have nothing to hide, most people are offended if they are denied the ability to keep certain personal information confidential. Crucial to one's sense of self is the right to maintain some decision-making power over what information to divulge, to whom, and for what purpose. The uses of new technologies are always threatening to overtake current law, leaving society without a new set of laws and social mores to limit and define the extent to which new devices can be used to know all we can about each other, often without regard to each other's wish to keep information private.

Recommendations

SUP10 ESTABLISH NEW CONTRACTING PROCEDURES FOR THE CONTINUED OCCUPANCY OF LEASED OFFICE SPACE
Simplify the procedures for renewing leases.

SUP11 REDUCE POSTAGE COSTS THROUGH IMPROVED MAIL MANAGEMENT
Encourage postage savings through the implementation of mail management initiatives. Allow line managers to manage their own postal budgets.

REENGINEER THROUGH THE USE OF INFORMATION TECHNOLOGY

IT01 PROVIDE CLEAR, STRONG LEADERSHIP TO INTEGRATE INFORMATION TECHNOLOGY INTO THE BUSINESS OF GOVERNMENT
Create a Government Information Technology Services working group to develop a strategic vision for the use of government information technology and to implement NPR's information technology recommendations.

IT02 IMPLEMENT NATIONWIDE, INTEGRATED ELECTRONIC BENEFIT TRANSFER
Design an integrated implementation plan for the use of electronic benefit transfer for programs such as Food Stamps and for direct payments to individuals without bank accounts.

IT03 DEVELOP INTEGRATED ELECTRONIC ACCESS TO GOVERNMENT INFORMATION AND SERVICE
Use information technology initiatives to improve customer service by creating a one-stop "800" calling service, integrated one-stop service "kiosks," and a governmentwide electronic bulletin board system.

IT04 ESTABLISH A NATIONAL LAW ENFORCEMENT/PUBLIC SAFETY NETWORK
Establish a national law enforcement/public safety data network for use by federal, state, and local law enforcement officials.

IT05 PROVIDE INTERGOVERNMENTAL TAX FILING, REPORTING, AND PAYMENTS PROCESSING
Integrate government financial filings, reporting, and payments processing, and determine ways to eliminate the need for filing routine tax returns.

IT06 ESTABLISH AN INTERNATIONAL TRADE DATA SYSTEM
Develop and implement a U.S. Government International Trade Data System in the Treasury Department.

IT07 CREATE A NATIONAL ENVIRONMENTAL DATA INDEX
Organize the implementation of a national environmental data index in the Commerce Department.

IT08 PLAN, DEMONSTRATE, AND PROVIDE GOVERNMENTWIDE ELECTRONIC MAIL
Improve electronic mail and messaging among federal agencies.

IT09 ESTABLISH AN INFORMATION INFRASTRUCTURE
Develop a Government Information Infrastructure to use government information resources effectively and support electroni government applications. Consolidate and modernize government data processing centers.

IT10 DEVELOP SYSTEMS AND MECHANISMS TO ENSURE PRIVACY AND SECURITY
Establish a Privacy Protection Board. Establish uniform privacy protection practices and generally acceptable implementation methods for these practices. Develop a digital signature standard for sensitive, unclassified data by January 1994.

IT11 IMPROVE METHODS OF INFORMATION TECHNOLOGY ACQUISITION
(see PROC 09, PROC10, PROC15, SUP04, and FM06)

IT12 PROVIDE INCENTIVES FOR INNOVATION
Retain a portion of agency information technology savings to reinvest in information technology. Promote performance-base contracting for information technology. Establish a governmentwide venture capital fund for innovative information technology projects

IT13 PROVIDE TRAINING AND TECHNICAL ASSISTANCE IN INFORMATION TECHNOLOGY TO FEDERAL EMPLOYEES
Establish a program to train non-technical senior executives and political appointees in information technology. Require managers of information resources to meet certification standards. Promote collegial assistance in using information technology. Include training costs as part of all information technology purchases.

RETHINKING PROGRAM DESIGN

DES01 ACTIVATE PROGRAM DESIGN AS A FORMAL DISCIPLINE
The President's Management Council should commission the development of a handbook to help federal managers understand the strengths and weaknesses of various forms of program design.

DES02 ESTABLISH PILOT PROGRAM DESIGN CAPABILITIES IN ONE OR TWO AGENCIES
Test the usefulness of the program design handbook and the value of program design as a useful discipline.

file privacy

Ongoing Privacy Activity -

After a number of years of little interest in privacy issues, a number of serious ongoing efforts

Legislative

Boxer/Moran Drivers' License privacy bill

Proposal would amend title 18 to prohibit motor vehicle departments from disclosing, without authorization, personal information about a licensee to the general public for reasons unrelated to the mission of the agency.

Currently, in 52 states, an individual can obtain anyone's name and address simply by providing a license tag number to a DMV and paying a nominal fee. This has benefitted stalkers, such as the man who gunned down actress Rebecca Shaefer after getting her address from the California DMV. Also benefits anti-abortion protestors who use information to picket and harass clinic patients and doctors.

Bill is not intended to impeded legitimate use of this information by courts, law enforcement or other governmental agencies. Also allows businesses to verify information when licensee has waived right to confidentiality. Would permit sale to direct marketing organizations provided individual has been given the right to opt out.

Simon Privacy for Consumers and Workers Bill - S. 984

Cosponsored by Rep Williams, this bill aims at curbing abuses of monitoring by prohibiting certain types of monitoring activities, such as monitoring in bathrooms, and limiting the locations and situations where monitoring could be conducted. It gives Labor broad enforcement authority. While the Administration supports the objective of the bill, we have a number of concerns about some of its provisions. Those concerns have been passed on to the Committee (see DOL letter). We understand that the drafters are working to incorporate our concerns and we will work with them as the bill evolves.

Cardis Collins Individual Privacy Protection Act of 1993, HR 135

Would amend title 5 to make modest improvements in the Privacy Act and to establish a permanent Privacy Protection Commission as an independent entity in the Federal Government. This Commission would study the data banks, automated data processing programs of both private and public organizations to determine privacy protection standards and procedures currently in force. Would make recommendations for proposed Federal State or local statutes, regulations, or procedures.

Congresswoman Collins has introduced this bill in past sessions. But it has gone nowhere [Rob's comment - Gellman says that Collins has a new crew and they are simply reintroducing it out of habit - no one knows anything about the issue]. It was referred to the

House subcommittee on Information, Justice, Transportation and Agriculture.

Medical Records Privacy - The last medical records bill was introduced at the end of the Carter Administration. It was opposed by both the AMA and the law enforcement and intelligence communities. There is a recognition this time that the issue is complicated and that the concerns of all constituent groups must be addressed.

Consequently, while there is work being done behind the scenes to lay a foundation for a legislative proposal - none has been put together yet.

Administration Activities:

National Performance Review Recommendations

The NPR made specific recommendations on protecting privacy and confidentiality of records. Specifically, the task group looking at these issues recommended that the President establish a Privacy Protection Board that would establish uniform privacy protection practices and acceptable implementation methods for these practices. The Board would also proposed legislation creating a permanent national Data Protection Board.

The Information Infrastructure Task Force (IITF)

The IITF, like the NPR, operated under the aegis of the Vice President. Whereas the NPR focus is primarily on improving government performance, the IITF has a broader nationwide mandate. It grows from the vision of the United States as "a seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at users' fingertips. Development of the National Information Infrastructure (NII) will change forever the way people live, work, and interact with each other." (from the National Information Infrastructure: Agenda for Action.

This effort is being chaired by Ron Brown, Secretary of Commerce and has three committees:

- o The Telecommunications Policy Committee.
- o The IITF Applications Committee, and
- o The Information Policy Committee

The Information Policy Committee is chaired by Sally Katzen, Administrator of the Office of Information and Regulatory Affairs. Under this Committee is a subcommittee that has a privacy mandate. This group has developed a workplan to investigate what policies are needed to ensure individual privacy in the NII, while recognizing legitimate societal needs for data, including those of law enforcement. The group is currently meeting with privacy experts to gather data as widely as possible. It intends to hold a public hearing later this year or early next. It will next develop proposed policies for ensuring privacy in the NII. It is also within the charter of the group to develop privacy legislative proposals.

We think that this group will carry out the intent of the NPR recommendations. Although the IITF privacy group will look much more broadly at privacy issues.

Medical Records Privacy

The Department of Health and Human Services has convened a task force on the privacy of medical records. Its report will be coming out soon. In addition, the administration's health care reform proposal will have a privacy component.

technology and enhanced management oversight also offer the opportunity for some solutions. There is increased awareness across the information and computer industry of the need for improved information security. This is evidenced by industry advances in the security of computer operating systems, access controls, and databases software with enhanced security features. Technology alone, however, will not provide a solution. What is needed is a national policy to which technological solutions may lend themselves.

Opinion surveys over the last decade show a growing public concern about a lack of control over their personal information. As the Clinton Administration implements its February 22, 1993 technology plan, Technology for American's Economic Growth, A New Direction to Build Economic Strength and in particular as the Administration moves toward a National Information Infrastructure in a global environment, there is a need and an opportunity to concurrently implement appropriate privacy policies to protect personal data.

PRIORITY ISSUES

Putting Protections Around a Moving Target

Previously a system of records was stable in nature. In an increasingly electronic environment, a system of records is dynamic, changing from day to day or minute to minute. With more data available, and the matching of records easier and more accurate, and with networking among systems of records more pervasive, how do we define that which is being protected and how do we attach protections to it?

Role of the Individual, Role of the Institution

In the past, it was a relatively easy process to require an agreement between an individual and an organization to determine who could use personal information and for what purposes. Now, people from many organizations will have the ability to call up records from many locations. Many will have no direct relationship with the individual who is the data subject. This changes the nature of obtaining the individual's consent before using their data for other purposes and raises the question of who will "own" the data of the future, how can informed consent be obtained and what legal controls will surround the access of data by third, fourth, fifth, etc. parties.

Security of Sensitive Data

Health care, financial, academic, government, employment, telephone, and other records could be accessed, linked, used and disseminated. Individuals vary in their levels of sensitivity to use of each type of data. Combined record systems, which develop a profile of a person are often viewed as more sensitive than

information from any singular data base.

Individual level of sensitivity will also vary depending on the proposed user of the data. Should there be stronger and distinct levels of access for more sensitive categories or users of information and how will these categories be defined? Are there levels of information security defined for the various sensitivity of data? Are information security policy standards required? How should operations be audited and accesses tracked? Who will monitor access and how will it be effectively monitored?

Use

The creation of any electronic system of records brings with it the possibility that the data could be used for reasons other that those for which it was originally intended. Not all alternative uses of information are inherently undesirable. The mere existence of certain data will bring with it an "irresistible use" of data beyond that for which it was originally intended. What statements of policy should govern the purposes for which data may be used and who should decide? What oversight mechanisms are necessary to ensure appropriate uses?

Identifiers

Some fear that the use of a standard personal identifier increases the ease and likelihood that records will be accessed, linked and distributed. Others argue that the accuracy of any system of records will be increased if a standard identifier is used, assuring that the data is attributed to the correct person as it enters the system. On balance, what concerns are raised by the use of a unique personal identifier and what constraints, if any, should be place on the use of them?

Legislation

Privacy is now addressed by a complex matrix of laws, state and federal. An analysis should be done of the potential harm to individual privacy created by an interactive information structure that crosses state and national boundaries. Is new federal legislation necessary and, if so, should it address the private sector or public sector or both? Should existing laws be amended?

Responsibility

Who should have the responsibility for seeing that privacy concerns are taken into consideration in evolving public policy development. Government? Corporations? Should each individual bear some responsibility for him or herself? Also who should be responsible for the enforcement of guides, rules or regulations? Is an oversight board needed and, if so, what would be its mandate, authority?

Public Education
Potential harm to individuals is difficult to address because it is difficult to catalog all potential uses of information in order to point out risks. In addition, it is possible that those harmed are never aware of it. How can we make the public partners in privacy protection by increasing their awareness of potential threats to their privacy?

Employee Training
In the interest of quality customer service, more and more data is put in the hands of front line personnel, for example, those who answer the phone. How can we protect records from employees who are not ethical, competent or trained? Should written corporate acceptable use policy statements on information dissemination be required?

MILESTONES

1. Identification of the scope and nature of individual privacy concerns and key issues that are likely to arise, nationally and internationally, as the Administration moves toward a national information infrastructure. Target date: [redacted].

2. Development of a statement of fair information principles and practices within the context of the national information infrastructure in a global environment. Target date: [redacted].

3. Determination of who should have the responsibility for implementing the principles and practices. Target date: [redacted].

4. Identification of gaps in current U.S. law from the national and international perspective. Target date: [redacted].

5. Identification of control mechanisms and practices such as technology, oversight boards, training, public education, industry voluntary programs, executive orders, new legislation. Target date: [redacted]

6. Preparation of a paper outlining recommended proposals for actions, policies, and legislation to protect the privacy of individuals while allowing for the reasonable flow of information. Target date: [redacted].

7. Drafting of proposed legislation, should that be necessary. Target date: [redacted] April 1, 1994 deadline.

NATIONAL COMMITTEE ON UNITED STATES–CHINA RELATIONS
777 UNITED NATIONS PLAZA, NEW YORK, NY 10017-3521 (212) 922-1385 TELEX: 4972799 NCUSC FAX: (212) 557-8258

TO: Dianna Pierce Fax 202-456-2215

FM: Donna Mutchell for Jan Berris DATE: Oct 21, 1993

Total Number of pages (including this cover sheet): 4
If you do not receive all material transmitted, please call at number above.

Message:

This is the information on the Delegation. Any questions, please don't hesitate to call us.

Donna Mutchell

MEMORANDUM FOR SALLY KATZEN

THROUGH: James B. MacRae, Jr.
Bruce W. McConnell
Katherine K. Wallman

FROM: Jerry Coffey
Maya A. Bernstein

SUBJECT: S. 984 "Privacy for Consumers and Workers Act"

You are scheduled to meet with David Rems of the Council of American Survey Research Organizations (CASRO) on September 14. CASRO is an association of 150 companies which seeks to promote the profitable growth of the survey research industry in an ethical and professional manner. It promulgates a code of standards to which its members much adhere, governing 85% of the private sector domestic research market. (See Attachment A for more information about CASRO.) The purpose of their visit is to share concerns about S. 984 and H.R. 1900, the "Privacy for Consumers and Workers Act," which would regulate the electronic monitoring of workers. S. 984 is sponsored by Senator Simon. There has been one hearing, and there is no Administration position.

The purpose of this memorandum is to inform you about the bill in preparation for the meeting.

The bill defines electronic monitoring very broadly as any recording of information concerning an individual's activities via any form of technology other than direct observation by another person. It covers employees in the public and private sectors, including Congressional employees. The bill would restrict the frequency, duration, location, and types of monitoring permissible; would give employees the right to review monitoring data on themselves; and would prohibit disclosures more strictly than the Privacy Act. We understand that the legislation was drafted by the Communications Workers of America (CWA) to protect telephone customer service workers. However, as drafted, its impact would be much broader.

CASRO has several concerns with the bill. In particular, the bill would prohibit the random monitoring of telephone interviewers, a practice widely accepted in the survey research community as the best method for ensuring unbiased and accurate survey results. Telephone interviewing is an effective and efficient form of data collection, but it is subject to significant risk of bias introduced by interviewer performance. The preferred method for controlling this risk is through quality

assurance programs based on random monitoring. The prohibition of random monitoring would affect Federal surveys using this methodology, and could compromise the accuracy of information on which policymakers rely to make decisions, such as the current population estimates, used to determine the allocation of Federal funds, or the unemployment rate. Because of its generality, the provision could also jeopardize other public and private sector uses of quality control monitoring, such as political polling, consumer and market surveys, or even medical testing.

OIRA staff members also have other concerns about the bills, including their scope and workability, conformance to privacy principles, effect on the law enforcement and intelligence communities, and internal consistency. A detailed discussion of our concerns is attached. (See Attachment B.)

ATTACHMENT 1 to memo to Sally Katzen

BACKGROUND ON CASRO

CASRO is an association of about 150 private survey research firms that account for about 85% of the U.S. survey research market. The association estimates this private sector research market to be about $3 billion per year, or about the same size as the combined budgets for all Federal statistical activities.

[This comparison is not precise since some Federal funds are spent to purchase services from CASRO companies.]

Through its mandatory code of standards, CASRO promotes ethical conduct with respect to both respondents and clients. These standards are strong on protection of respondent confidentiality and avoidance of deceptive business practices.

[CASRO standards not do extend into some areas of methodology -- some CASRO companies compete in market niches that do not demand rigorous statistical designs. In these cases the CASRO standards only require that the client be informed of the specific methods used. However, many CASRO companies are contractors for Federal surveys and their methods fully meet OMB standards.]

In 1992, CASRO, together with some related organizations and many of their corporate survey clients, established a second group known as the Council for Marketing and Opinion Research (CMOR), charged to address two problems: restrictive legislation and declining respondent cooperation.

[CMOR was created in response to an explosion of bills that would restrict survey methods (over 400 Federal and State proposals in 1991). CASRO attributes much of this legislative ferment to abuses of survey methods for purposes other than research, e.g., telemarketing schemes masquerading as research. CASRO has also experienced a decline in respondent cooperation in legitimate research which it attributes to the same deceptive practices.]

ATTACHMENT B to Memo to Sally Katzen

Detailed discussion of S.984

NOTIFICATION PROVISIONS

Employee notice. The most generally problematic provisions in the bill require an employer to provide specific notice of the hours and days per calendar week that electronic monitoring will occur (Section 4(b)). This would defeat the purpose of monitoring for its most common applications: discovering problem employees, conducting survey research, and ensuring the security of information systems.

First, employees who tended to act in an unlawful, unprofessional, or unethical manner would hide such behavior during those times when monitoring was being done.

Second, interviewers conducting opinion research would inevitably be more cautious and conscientious at the times when monitoring was being carried out than at other times, defeating the control function of monitoring. Survey designers must conduct random monitoring without disturbing the ongoing data collection process in order not to change the behavior of interviewers which might distort the data they must obtain. If random monitoring could not be conducted, opinion researchers would not be able to determine whether calls were actually being made, interviewers fully understood all aspects of the survey or required further training, interviews were being conducted properly or, answers were being properly recorded. This would severely erode the quality of opinion on which the Government relies for policy information, such as the Current Population Survey or the National Household Education Survey. It would also affect election polling and market surveys.

Finally, providing advance notice of monitoring would defeat the purposes of information systems security monitoring. A common method for ensuring computer security is to create a "profile" of a typical user of a system by monitoring normal work patterns, and then to monitor for deviations from the profile which would indicate suspicious activity, such as an intruder, or an employee exceeding authorization. Since the monitoring would be subject to advance notice and could not be relied upon to provide a true picture of users' actual information security practices, such profiles would be useless.

General notice should be sufficient to inform employees or applicants that their work will be monitored from time to time, the type of information collected, and the purposes for that monitoring.

Customer notice. The bill also requires specific notice be given to customers calling businesses or members of the public calling

Federal agencies if they may be monitored.

Section 4(d) requires employers to notify customers that they may be monitored as part of telephone service observation by recorded or automated attendant, or, if the employer does not use such a device, in the customer bill. This provision does not allow for the possibility that a human being could give such notice over the phone at the beginning of a call, as is a common practice for some police or fire departments. While the provision is designed to ensure notice, it would allow transactions to occur without notice, as when a customer places an order by phone and is billed subsequently. This seems contrary to the goals of the bill.

Section 4(f) requires Federal agencies to provide the public with notice of monitoring and the opportunity not to participate. For similar reasons as stated above, this provision would affect the accuracy of opinion surveys by changing the behavior of respondents and thereby distorting data. The survey industry claims in letters to Senator Simon that monitoring of telephone interviewers is random, only includes a portion of any particular interview, and that data are not associated with particular interviews. They further state that even if data were associated with a particular individual, supervisors who conduct monitoring are bound by the same rules of confidentiality that bind interviewers. Therefore, monitoring is unlikely to threaten the confidentiality of survey data or privacy of the respondents.

SCOPE and COVERAGE

The scope of the bill is overly broad in prohibiting certain types of monitoring, and overly narrow in its exceptions.

Periodic and random monitoring. Section 5(a) allows for "periodic or random" electronic monitoring in certain cases, but the meaning of "periodic and random" is not defined in the Act. This section implies that such monitoring may be conducted without prior notice, even though section 4(b)(3) requires prior notice. This should be clarified.

Section 5(b) This section allows "periodic and random" monitoring of new employees for 60 days, work groups up to two hours per week, and other employees up to five years. This section implies that those employed at passage of the Act may continue to be monitored up to five years, but those newly hired may only be monitored for the first 60 days of their employment, which doesn't make sense. It is not clear what the drafters intended.

Further, limiting the monitoring of employees based on seniority is not fair nor necessarily wise. Even though veteran telephone service or solicitation workers may be more capable in conducting their work, there are several reasons to include them in monitoring programs. Their experience may make them more adept at circumventing proper procedures. "Burn-out" may cause

diminished attention to detail and inappropriate behavior toward customers, and these circumstances may increase, rather than decrease, with experience. Further, survey interviewers must be subject to monitoring for each new survey, no matter how long their experience in interviewing. Each survey has its own sampling and respondent selection rules, questionnaire, and software which support the procedures. Every survey must be monitored in the beginning of the data collection to ensure that it is carried out according to its intended design.

Employer access. Section 9 allows an employer, in the employee's absence, to gain access to alphanumeric data for which the employer has an immediate business need, as long as the employer does not use the data for the purpose of discipline or performance evaluation and later informs the employee that the data were obtained. It is not clear why this provision is limited to alphanumeric data only. It specifically excludes "data obtained by the aural or visual monitoring" of employees or the "interception of the [employee's] communications, visual images, audio impressions, or data that can be used to create visual or auditory information. This provision would prevent the supervisors of computer graphics programmers or medical technicians from gaining access to visual images employees create or use as a regular part of work.

CIA argued in a report on the bill sent to Senator Simon, that "any information maintained in Federal information systems is the property of the Federal government and must be accessible at all times to authorized personnel for the performance of official duties." We disagree with such a sweeping statement, since some incidental uses of information systems should be allowed to make workers more efficient and maintain good morale. For example, GSA allows certain incidental uses of the telephone which are unrelated to an employee's work, such as arranging child care or contacting businesses only open during the work day. It is possible that similar uses of an electronic mail system would be permissible, but there is a lack of policy in this area. Federal employees do have some expectation of privacy in the contents of their desk drawers and on the phone, and it may be that such expectations should extend to electronic systems. In the absence of policy or legal guidance, it is inappropriate to assume that Federal agencies should treat all electronic information as their property with unlimited access. However, it is both reasonable and necessary that supervisors should have access to information which they require to perform their assigned duties. Balanced language should be drafted to achieve these policy goals. This section also requires an employer to give notice within a reasonable time after accessing an employee's files. We disagree with CIA's claim that providing such notice would be a great burden on the efficient performance of government operations.

Non-work activity. Section 10(a) limits monitoring other than that which is confined to an employee's work. [This is also law enforcement and intelligence related.] Intelligence agencies

have a special problem with this provision as it would prevent them from using some techniques which are now allowed by law, such as polygraph interviews of applicants and employees, which typically include questions about individuals' habits outside of work. It would also prohibit monitoring of Federal employees under suspicion of espionage, since those activities are not "confined to the employee's work," nor covered by the section allowing monitoring under warrant. Foreign intelligence warrants are not covered by the law cited.

Computer systems' security could be compromised if only monitoring of employee's work is allowed. Obtaining a warrant to observe an intruder or an individual exceeding authorized access requires showing evidence of suspected wrongdoing, but obtaining that evidence would be a violation of section 10, since it would be monitoring other than the employee's assigned work.

Prohibited locations. Section 10(b) prohibits collecting information in certain private places, such as bathrooms or dressing rooms. However, it does not prohibit monitoring in other particularly private places such as medical examining rooms, nor in other places where employees do not perform work, such as cafeterias or gyms (except for those who actually work in the cafeteria or gym).

Definitions. The definitions of "employer" and "employee" are recursive and therefore not very useful.

The definition of "electronic monitoring" is so broad as to include any machine-recorded observation conducted by any means other than direct observation by another person.

The definition of "personal data" includes only examples of data stored on paper, e.g., "printouts" but not magnetic, optical, video, or audio media.

CONSISTENCY WITH PRIVACY PRINCIPLES

The bill does not conform to certain established privacy principles, and limits disclosures more strictly than the Privacy Act of 1974.

Access and amendment of records. Section 7(a) grants employees the right to a review or copy of all personal data collected by electronic monitoring. However, it does not confer the complementary right to amend records which are not accurate, relevant, timely, or complete--a right individuals have under the Privacy Act.

Authorized disclosures. Section 10(d) prohibits the disclosure of personal data obtained by electronic monitoring except with the subject employee's prior written consent, with four exceptions. These exceptions are much narrower than those

allowed by the Privacy Act, and are probably unworkable and inadvisable. For example, the following disclosures would be prohibited:

- to the Department of Justice when it defends an agency
- to a law enforcement agency without a warrant or subpoena
- to any other agency without a court order
- to a contractor performing monitoring services for an employer
- to a Member of Congress acting on behalf of a constituent
- to a Congressional Committee or the Comptroller General
- for academic or personnel research

In a draft letter to Senator Simon, NSA objected to the provision since it might require the written consent of an employee for interagency disclosures. OIRA staff disagrees with NSA's argument. Not even the Privacy Act of 1974 allows unlimited interagency transfers of information, although certain disclosures are permitted. NSA further objects that the narrower disclosures of the bill conflict with disclosures permitted under the Privacy Act and leave doubt as to which bill is controlling. The bill does not conflict with the Privacy Act; it is merely more restrictive. Many statutes provide for more stringent limitations on disclosure than the Privacy Act, such as statutes restricting the use of employee drug test results or Census data. If a particular statute limits disclosures to certain circumstances, then the agency has no discretion to disclose under section (b) of the Privacy Act, except in the enumerated circumstances of the more restrictive statute. A policy level decision must be made as to whether strict limitations on the disclosure of monitoring data is appropriate.

LAW ENFORCEMENT AND INTELLIGENCE

Section 7(b) provides an exception to employee review of monitoring records for investigations of civil or criminal law enforcement, willful gross misconduct, or conduct which would have a significant adverse effect involving economic loss or injury to the employer. However, the employer must provide review if such investigation has been completed, or if disciplinary action has been initiated. It is not clear why a completed investigation, which may lead to prosecution or other action must be disclosed prior to referral to the prosecuting agency. Further, this provision would require the disclosure of confidential source information. Congress recognized, in the Privacy Act of 1974 (5 USC 552a) and the Freedom of Information Act (5 USC 552), the legitimate need for agencies involved in law enforcement activities to protect the integrity of their investigations and the identities of confidential sources by allowing exemptions from its disclosure provisions. A similar provision would be appropriate.

CIA and NSA have requested exemption from all provisions of the bill for the intelligence community and its contractors. However

there are provisions from which they do not require exemption and should be subject if the rest of the Federal government is subject. For example, a requirement to give notice to applicants at the first interview of the types of monitoring the agency performs, or general notice and posting requirements about the types of information collected and the purpose for the collection would not jeopardize the intelligence community and would be appropriate.

E X E C U T I V E O F F I C E O F T H E P R E S I D E N T

20-Oct-1993 03:47pm

TO: John Podesta

FROM: Robert N. Veeder
Office of Mgmt and Budget, OIRA

CC: Maya A. Bernstein

SUBJECT: IIA

Attached is a rackup (wrackup?) of current privacy state of play in congress and with the administration. Would be useful to have you endorse the work of the IITF privacy working group as fulfilling the National Performance Review privacy reccs. Call me with q's. Otherwise, break a leg.

PS, I included nothing about the state of play on the EC directive. But, there appears to be dissension over what it should loo The French want it stronger; the Brits want it weaker. It doesn't look like they'll get their act together soon (e.g., within the next two years. We'll know more after the ad hoc group meets in Paris next month. Wendell Albright, State Department, is leading the US contingent. I'll let you know.

A PC Data File is attached. Use PCT SAD to download to your PC

E X E C U T I V E O F F I C E O F T H E P R E S I D E N T

20-Oct-1993 01:30pm

TO: John Podesta

FROM: Maya A. Bernstein
Office of Mgmt and Budget, OIRA

CC: Robert N. Veeder

SUBJECT: S984/HR1900 "Privacy for Consumers and Workers Act"

John --

I understand from Rob that you are speaking at IIA on privacy and need some information about the workplace monitoring bills. I am the OIRA lead staffer, and Rob suggested that I send you some materials.

I sent the attached memo to Sally in preparation for a meeting she had with lobbyists from the survey research community, so the cover memo has that kind of bent. However, the attached analysis (probably much more than you need) covers all of the major issues OIRA has with the bill. Sally also met more recently with representatives of the National Association of Manufacturers, DMA, and other organizations representing employer issues.

Some more recent background than is in the attached memo:

S.984 was introduced by Sen. Simon (D-IL), chair of the subcommittee on Employment and Productivity (Comm on Labor) and by Rep. Williams (D-MT), chair of the subcommittee on Labor-Management Relations (Comm on Education and Labor). The Senate subcommittee held a hearing in June at which the Administration declined to testify as there was no Administration position at that time. We agreed to send written reports instead.

The Senate subcommittee wrote letters asking the intelligence community for their opinions, but no other agency. We advised CIA and NSA to send letters narrowly focused on intelligence issues (CIA explained their problems with the bill and asked for an exemption) leaving the larger issues to a more appropriate lead agency.

Many agencies have significant problems with the bill, but we had a very difficult time getting any of them to submit reports. Finally, in preparation for a Senate markup scheduled today (later cancelled) and House markup still scheduled for the first week in November, Dept of Labor sent a report, and many agencies commented, but Labor refused to incorporate any comments related

to employer issues, including comments from their own Bureau of Labor Statistics.

[In the meantime, we discovered that the two subcommittees are working on new drafts which they have not shared with us, and on that basis HHS refused to clear/send a letter they had prepared.]

Knowing that IRS and SSA do significant monitoring of their employees (and probably other agencies such as Nuclear Regulatory Commission), that Census and the statistical agencies have significant concerns about the bills' effects on the accuracy of statistical data, and that Justice has serious reservations about giving Dept of Labor enforcement and independent litigating authority, we felt it irresponsible to allow Labor to send a letter which did not address these issues as the Administration position. Therefore, Sally suggested sending a letter which merely stated that we agree with the goal of curbing monitoring abuses and protecting the legitimate privacy rights of individuals, that we have significant concerns about the current bill but we understand other drafts are in the works, and that we would be happy to work with the Committees as the legislation evolved. She recommended sending no specific substantive comments at this time. [My understanding is that she talked with you about this position in advance, or that you talked with Bruce McConnell, my boss.] Labor sent such a letter yesterday.

The two issues Sally finds most persuasive are 1) that the bill would prohibit random monitoring, the standard industry practice in survey research for eliminating bias, and 2) the argument that the bill would impede the monitoring of regulatory compliance of various sorts, including safety. You should know that some of the other arguments about the bill are quite extreme, including that because the definition of "electronic monitoring" is so broad, the bill would limit or prohibit the use of email--by sending and receiving email, one is recording and transmitting information about work activities (i.e. that someone was logged in and using email at a particular time).

The bottom line is that I don't think the bill is going anywhere in this Congress, even if Simon continues to push it. We hear that Chairman Ford doesn't like it; Chairman Kennedy is lukewarm. Subcommittee staffs are working together to improve the bill, and we hear they are talking informally to some agencies (HHS, DOJ), so even though we did not send specifics in the Labor letter, they are aware of many of these issues.

I will be happy to send you copies of the bills, the new draft which we have informally (and which is not yet introduced) the Labor letter, other agencies' comments, or anything else you might find useful. Please feel free to call me if you have any questions or I can help in any way. x4816 --- Maya

Task Force Efforts

- Meeting with representatives from
  - Professional associations
  - Insurance community
  - Law community/hill
  - Technology and data management areas
  - Vendors
  - Credit associations
  - Media
  - Privacy Advocates
  - Research community
  - Other Privacy Studies (IOM)
- February 1993 conference "Health Records: Social Needs and Personal Privacy"
- Final report:
  - Review copy: Sept 1993
  - Final report: Winter 1993

456-2715

HHS Task Force on the Privacy of the Private Sector Health Records

- The Task Force was established in 1990
- Initial charge:
  - examining the extent to which there are problems with the use of personally identifiable medical and other health-related records in the private sector;
  - identifying what needs for health information exist in the public and private sector;
  - reviewing current laws and practice related to the privacy of private sector health records.
  - recommending steps that the Federal government, could if problems were identified, appropriately pursue to protect nonfederal record systems.
- Emerging events have refocused mission:
  - examine efforts to develop health care information systems in the context of health care reform and other efforts to develop electronic health information networks.

BOSSES WITH X-RAY EYES

Your employer may be using computers to keep tabs on you

BY CHARLES PILLER

Each and every day, Gayle Grant and her colleagues were electronically monitored down to the second as they did their jobs. Unplugging themselves from their job monitors could lead to dismissal. "We punch in and out of three units: the time clock, the VDT [computer terminal], and the telephone keypad known as Collins. We plug a phone jack into Collins that is attached to our headset and [we] receive telephone calls. The VDT and Collins track every second of our day," says Grant (a pseudonym), an airline reservations agent in California. She and her colleagues were allowed 11 seconds between calls and 12 minutes of personal breaks daily. Two episodes of unauthorized unplugged time in a week were cause for disciplinary action. She eventually cracked under the pressure. Grant suffered a nervous breakdown.

Grant's reaction may have been extreme, but her employer merely followed standard practice in many industries, and acted consistently with both the letter and intent of U.S. federal law. The 1986 Electronic Communications Privacy Act (ECPA) prohibits phone and data-line taps with two exceptions: law-enforcement agencies and employers.

The police or FBI can tap lines—but only as a last resort under court order—to crack criminal conspirators, drug traffickers, and other serious-crime suspects. The courts permit fewer than 1000 such taps each year, nationwide.

Employers have no such limits. They may view employees on closed-circuit TV; tap their phones, E-mail, and network communications; and rummage through their computer files with or without employee knowledge or consent—24 hours a day.

The most pervasive use of monitoring takes place in occupations where tasks are highly repetitive, so productivity can be easily measured. The Communications Workers of America, the union that represents most telecommunications workers, estimates that employers eavesdrop on phone calls between workers and consumers 400 million times per year—more than 750 calls every minute. Mail sorters, word processors, data entry clerks, insurance adjusters, and even computer tech-support specialists, often working on terminals connected to a mainframe, may be monitored constantly or intermittently for speed, errors, and time spent working.

Working in Glass Offices

MOST PROFESSIONAL AND TECHNICAL EMPLOYEES assume that they have nothing to fear. Their privacy is protected by the nature of their jobs—too complex to evaluate by machine, right? To test that assumption, *Macworld* examined 25 popular network-management, integrated groupware, electronic-mail, and remote-access products to see if they could be used to invade employee privacy, and if so, how easily. The study used only Macintosh software, but similar tools are available on other platforms.

If your office network runs on a full-featured network operating system, like Novell NetWare or Microsoft LAN Manager, and is run by a technically astute manager, then your Macintosh and all data transferred from it is an open book. Working from an office across the room or across the country, a network manager—particularly in server-based local area networks—can eavesdrop on virtually every aspect of your networked computing environment with or without your approval or even knowledge. The manager can view the contents of data files and electronic-mail messages, overwrite private pass-

MICHELE CLEMENT

Job Seeker Beware: Electronic Hurdles to Employment

Ross Perot's eager campaign volunteers were stunned last year when they discovered that agents of the billionaire politician may have looked into some of their backgrounds. The news stimulated an FBI probe into allegations that the Perot campaign organization illegally obtained volunteers' confidential credit reports. The allegations made Perot seem paranoid and sleazy. Actually, he may just have been following the standard practice of many prudent managers, who have become some of the biggest users of electronic tools to investigate job seekers or recent hires.

VIRGINIA LIBERATORE

Tom O'Neil, a New Jersey business consultant and onetime chairperson of the Perot campaign in his state, claims he was confronted by representatives of Perot's Dallas headquarters who had obtained error-ridden versions of his personal data.

These managers verify prior-employment claims carefully, of course. Nothing new there. Then they check credit and criminal records online in a matter of minutes. If data is not available in electronic form—for example, college transcripts—they hire research services to get transcripts and deliver their contents to the client's online account in a day or so.

These efforts fit right into a corporate culture that leads a growing number of employers to require drug tests and, leaving nothing to chance, so-called personality profiles. Such profiles may contain hundreds of true-false questions, such as these typical examples: "I have read little or none of the Bible," "My sex life is satisfactory," and "I am very seldom troubled by constipation." They may be used to predict laziness, poor work habits, or psychological problems, or merely to verify whether the job seeker has mainstream values or an outlook consistent with company goals.

"Management is very pragmatic," says Alan F. Westin, a professor at Columbia University who is an expert on electronic privacy issues and an industry consultant. "Management will do whatever the social system and the legal system says, with a special emphasis on whether it helps get the work done to make a better product."

This pragmatic approach derives, in part, from skyrocketing health-insurance and legal bills. The cost of medical care has led many employers to screen out applicants who smoke or are overweight.

And until last summer, many employers searched online data banks to find out whether a job seeker had ever filed a workers'-compensation claim—an insurance claim for an on-the-job injury. Some employers refused to offer a job to anyone who had ever filed a comp claim. The Americans With Disabilities Act, signed into law last year, limits the use of such data banks before a firm offer of employment has been made. But if an employer finds a history of compensation claims after making a job offer, the employer can shift the prospective employee to a job classification that reduces risk of reinjury. If in the employer's opinion no appropriately safe job is available, the offer can be rescinded.

And a rash of lawsuits in the 1980s accusing employers of "negligent hiring" has also pushed employer vigilance to a new standard. You hire a man to do maintenance at your hotel, giving him a passkey to all the rooms, of course. That man rapes a guest. Because you failed to check his criminal history online, you didn't know that he served time for assault six years earlier. Welcome to court. Employers are caught in a dilemma, says Westin. "Do they stay with the hands-off, respect-the-privacy, that's-not-our-business view, or do they respond to their lawyers' warnings to protect themselves against liability, and their bean-counters' warnings that health-benefit costs are going to be out of sight?"

Employers have a responsibility to protect themselves from potential liability and their customers from undue danger. But privacy advocates ask whether society is well served by a business culture that can blacklist people with the cool efficiency of a 9600-bps modem.

words, and audit your time and activities on the network.

All the major electronic-mail and groupware products that combine messaging, file management, and scheduling (such as WordPerfect Office) allow the network administrator to change passwords at any time, then read, delete, or alter any messages on the server. With few exceptions, network-monitor programs, such as AG Group's LocalPeek, Farallon Computing's Traffic Watch II, and Neon Software's NetMinder, allow astute managers to read files transmitted over the net. In short, these tools are only slightly less invasive than others specifically designed for surveillance and used primarily on mainframe systems.

They Like to Watch

NETWORK ADMINISTRATION AND COMmunication tools were designed for valid reasons, not to invade employees' privacy. Like any technology, they are value-neutral. Some vendors even include strongly worded privacy warnings and a few offer options that allow a client Mac to shut out network managers.

The capacity to snoop is there, but is it used? Old surveys and anecdotal accounts suggest that in some industries—telecommunications, insurance, and banking, for example—as many as 80 percent of employees are the subjects of telephone or computer-based monitoring. Such estimates may be inflated, but there is little dispute that many employers monitor routinely. And if the rapid sales and market growth of snooping tools is an indication, monitoring is on the rise. But virtually no rigorous research has been done about how much electronic eavesdropping takes place on the job.

Until now. *Macworld* conducted a survey of CEOs and MIS directors at 301 large, medium, and small businesses in a wide range of industries to find out how much they peek at their employees' work on their computers, and why (see the "Electronic Eavesdropping at Work" charts). About 22 percent of our sample have engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications. In companies with 1000 or more employees, the figure rises to 30 percent. Nearly 16 percent of respondents report that they have checked employees' computerized work files.

The average company in our study employs 3240 people, so the total sample represents the conditions experienced by nearly 1 million workers. This data suggests that some 20 million Americans may be subject to electronic monitoring through their computers (not including telephones) on the job. Meanwhile, only 18 percent of respondents' companies have a written policy regarding electronic privacy for employees.

Managers who endorse electronic surveillance argue that it helps them gauge productivity and chart the work flow of a group of employees. It can generate statistics on individual or departmental accomplishments and plot future work loads. Computer monitoring can even be used to give employees managerial feedback and reduce the need for personal attention from supervisors. In the

MANUELLO PAGANELLI

Privacy advocate Marc Rotenberg: Contrary to what many people believe, "E-mail is more like a postcard than a sealed letter."

MANUELLO PAGANELLI

Senator Paul Simon: "Employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work."

VIRGINIA L'BERATORE

Privacy expert Alan F. Westin: "Monitoring that creates feelings of surveillance and stress is antithetical to the new cultures of management."

Macworld survey, 12 percent of responding employers endorse monitoring for evaluating performance or productivity.

Monitoring can also increase safety or adherence to company rules, some employers contend. Some trucking companies, for example, set on-board monitors to record speed, engine-idling time, and length of stops. The system ostensibly tries to ensure that truckers drive safely and take adequate rest breaks.

Companies that deal in sensitive data may feel compelled to guard against disloyal or merely careless employees who might divulge it to competitors (see the sidebar "To Catch a Spy: Is Workplace E-Mail Private?"). And 4 percent of our survey respondents endorse electronic monitoring "for routinely verifying employee honesty." A much higher number—23 percent—feel electronic monitoring is a good tool where reasonable evidence of wrongdoing, such as theft or negligence, comes to light.

While nearly half of the managers in our survey endorse the concept of electronic monitoring, and nearly a fourth actually conduct electronic monitoring, most of those don't do it often. About 71 percent of those who conducted such searches did so only five or fewer times in the preceding two years. Only two companies had searched employees' work files, voice mail, electronic mail, or networking communications more than 100 times during that period.

A Model Employment-Privacy Policy

Macworld's privacy survey suggests that less than one-fifth of U.S. employers have electronic privacy policies. So in most cases, employees may have no idea whether or how employers monitor their everyday activities and work files. The following points represent what many privacy advocates consider basic features for a good electronic-privacy policy for employers:

- Employees are entitled to reasonable expectations of personal privacy on the job.
- Employees know what electronic surveillance tools are used, and how management uses the collected data.
- Management uses electronic monitoring or searches of data files, network communications, or electronic mail to the minimum extent possible. Continuous monitoring is not permitted.
- Employees participate in decisions about how and when electronic monitoring or searches take place.
- Data is gathered and used only for clearly defined work-related purposes.
- Management will not engage in secret monitoring or searches, except when credible evidence of criminal activity or other serious wrongdoing comes to light.
- Monitoring data will not be the sole factor in evaluating employee performance.
- Employees can inspect, challenge, and correct electronic records kept on their activities or files captured through electronic means.
- Records no longer relevant to the purposes they were collected for will be destroyed.
- Monitoring data that identifies individual employees will not be released to any third party, except to comply with legal requirements.
- Employees or prospective employees cannot waive privacy rights.
- Managers who violate these privacy principles are subject to discipline or termination.

From Watching to Intruding

THE *MACWORLD* SURVEY INDICATES THAT many employers may recognize that excessive monitoring has possible negative side effects. "Technology now allows employers to cross the line from monitoring the work to monitoring the worker," Cindia Cameron, a field organizer for 9 to 5, National Association of Working Women, told a Senate committee. She cites the case of an express-mail company employee whose computer logs the length and frequency of her trips to the bathroom. The woman was reprimanded for using the bathroom four times in a single day.

Some employers use monitoring data in efforts to boost productivity through competition—by posting data publicly. One enterprising Florida company, Thomas Powell Associates, found a way to automate the process. "I got the idea watching the [Miami] Dolphins [football team]," says a company founder. "Those athletes play their hearts out. Why? Certainly the money helps, but it's not the real reason. They play at 100 percent because everything they do is seen by hundreds of thousands of people—instantly." The company produces and sells software that instantaneously puts every telephone operator or telemarketer's productivity statistics on a computer screen, visible to all employees.

Do such schemes pay off? "Monitoring that creates feelings of surveillance and stress is antithetical to the new cultures of management that our society is moving toward," says Alan F. Westin, a professor at Columbia University and consultant to the data-gathering giant Equifax. Westin practically invented the idea of "electronic privacy" and has written on the subject for three decades. "[If management] doesn't motivate employ-

To Catch a Spy: Is Workplace E-Mail Private?

Most people believe that electronic-mail messages are secured by a personal password—as private as a letter in the U.S. mail. "They are finding out," says Marc Rotenberg, Washington, D.C., director of Computer Professionals for Social Responsibility, "that E-mail is more like a postcard than a sealed letter."

Symantec's Eugene Wang, who stands accused of theft of trade secrets, is at the center of a bitter debate over the privacy of commercial E-mail services that are used for company business.

Test case for privacy Employers have ready means to read E-mail messages, and many do just that, as computer executive Eugene Wang found out recently. His case, involving two Silicon Valley companies, could break new ground in electronic-privacy law.

Wang, who was Borland International's vice president for computer languages, defected to a direct competitor, Symantec Corporation, last September. Court documents filed by Borland attorneys state that shortly after Wang announced his departure, Borland execs found E-mail addressed from Wang to Symantec CEO Gordon Eubanks. The messages allegedly revealed top-secret corporate data, including marketing plans, product-release dates, and detailed information on Borland's game plan against Symantec. The police and FBI were called in shortly thereafter, and seized other documents at Eubanks' and Wang's homes.

Because Wang used MCI Mail—a commercial E-mail service—allegedly to transfer data to Eubanks, electronic privacy has become a key issue in the case. Wang and Eubanks, who have been indicted on criminal felony charges involving theft of trade secrets, deny that they violated trade secrecy laws. They also argue that when Borland viewed Wang's MCI Mail messages, the company may have violated federal law. If so, the confiscated E-mail messages might not be admissible in court. The 1986 Electronic Communications Privacy Act (ECPA) protects messages sent on commercial E-mail, such as MCI Mail, from outside or unauthorized users. "Even if Borland had gathered evidence in a legitimate and legal way regarding privacy, [Eubanks and Wang] would still be innocent," says Symantec attorney James McManis. "But if after reviewing all the data, it appears to us that there has been a violation of the (ECPA) statute, we will raise that."

Borland counters that it paid for Wang's MCI Mail account, and therefore had every right to inspect the messages. "New employees at Borland are given an MCI [Mail] password that is on file with a Borland administrator," says Borland spokesperson Steve Grady. "You do not have a reasonable expectation of privacy in an E-mail system that is given to you for company business by your employer." If the privacy issue is litigated, it could set new standards on the privacy of commercial E-mail.

California challenges Federal rules regarding in-house electronic mail are less ambiguous than those governing commercial E-mail. ECPA treats internal company communications as company property. And a *Macworld* survey suggests that some 375,000 employers agree. About 9 percent of respondents—CEOs and MIS directors of U.S. companies of all sizes—indicate that they sometimes search employee E-mail files. This prerogative is being challenged in California, where the state constitution specifically protects privacy, unlike the U.S. Constitution. Court documents indicate that Alana Shoars, formerly E-mail director of Epson America, claims she was fired in 1990 for questioning her boss's right to read hundreds of E-mail messages sent between other employees. Shoars filed wrongful-termination and class-action lawsuits against Epson. Her attorney, Noel Shipman, claims that by reading employee E-mail messages, Epson violated both the state constitution's privacy provision as well as a California eavesdropping statute.

Shipman also represents two employees of Nissan Motor Corporation embroiled in an E-mail controversy. Rhonda Hall and Bonita Bourke were allegedly fired from their jobs installing software and training other employees. A legal brief filed by Shipman claims that the two were fired or forced to resign after complaining about managers printing and reviewing printouts of personal messages from the company's E-mail system—messages they assumed were private. The two sued for invasion of privacy and wrongful termination.

Both the Nissan and Epson cases were dismissed by lower courts, but are now on appeal. If the plaintiffs prevail in either situation, the legal status of personal E-mail messages on internal company systems will be thrown open, perhaps resulting in greater privacy rights.

ees to be more participative, to be more committed to the workplace, then the chances of producing the kind of quality work that will compete with the Japanese and the Germans are very low."

And managers concerned with both productivity and containing health-insurance costs may find electronic monitoring to be self-defeating. Electronic monitoring increases employee "boredom, tension, anxiety, depression, anger, and fatigue," according to a recent study of 745 employees of telecommunications companies, jointly conducted by researchers from the University of Wisconsin and the Communications Workers of America. These findings confirm earlier studies that implicate electronic monitoring as a major workplace stress factor—linked, in part, to the sense of powerlessness that monitored employees feel.

Possible Legislative Relief

SUCH CONCERNS HAVE STIMULATED some members of Congress to ask what constitutes fair and appropriate monitoring. The proposed Privacy for Consumers and Workers Act failed in the last Congress, but Capitol insiders have high hopes for it in this session. The proposed law would limit how monitoring could take place in these ways:

- Employers would have to tell new hires how they might be monitored and how the collected data would be used.
- Employers would be required to give advance warning that monitoring will take place (except for employees on probation)—possibly including a signal light or beep tone during monitoring.
- The total time that an employee could be monitored would be capped at two hours per week.
- Secret, periodic, or random monitoring of long-term employees would be prohibited.

Macworld's survey shows that the law would force policy changes for many businesses. We found that only 31 percent of companies that conduct electronic monitoring or searches of employee computers, voice mail, electronic mail, or networking communications give employees advance warning.

Many companies recognize consumer demand for privacy protections, and they have stepped forward with pioneering consumer-privacy policies that go far beyond the limited legal requirements. But few companies have policies in place that go as far to protect employee privacy as the Privacy for Consumers and Workers Act would mandate.

Companies that have led the way on consumer-privacy concerns, such as American Express, Citibank, and Equifax,

describe their electronic monitoring of employees as strictly limited. But they would not release internal policies on employee privacy, and they acknowledged surveillance practices beyond what would be allowed by some features of the congressional proposal.

One reason that employers may give less weight to employee privacy is that they feel countervailing pressure: legal requirements to monitor or audit employee activities, particularly in information-intensive industries. So most employers comply with employee-monitoring laws and regulations as they see fit, rather than breaking new ground by minimizing monitoring and using the least-invasive approach, says privacy expert Westin.

Industry groups also castigate the Privacy for Consumers and Workers Act. "An employer would be put in the absurd position of having to advise suspected thieves when they are being observed," Vincent Ruffolo, president of Security Companies Organized for Legislative Action, told a Senate hearing.

If the proposal is enacted, says Lawrence Fineran of the National Association of Manufacturers (NAM), customer service will erode, and manufacturers might have to abandon certain kinds of computer-aided manufacturing. "NAM opposes any legislation that will interfere with the ability of modern and future equipment that can assist domestic companies in their fight to remain competitive," Fineran says. "Otherwise the United States may as well let the information age pass it by." Yet Japan and most of Europe already impose much tighter restrictions on employee surveillance than the U.S. proposal would mandate.

Few privacy advocates argue that monitoring should be eliminated. But they say industry ignores a critical factor: most employees are hardworking and honest. "The problem with the business community," says Louis Maltbe, director of the American Civil Liberties Union's Workers Rights Project, "is that they are trying to make the rules with the assumption that every employee is a goldbrick."

Maltbe and other advocates see reasonable privacy protection going far beyond the provisions of the proposed law, to the point where employees have some control over monitoring practices and data collected (see the sidebar "A Model Employment-Privacy Policy").

"There has been kind of a reflex reaction, automatically resisting things that ultimately have been very helpful to industry," says Senator Paul Simon, D-Ill., principal sponsor of the Senate version of the privacy bill. "The banking industry resisted having—believe it or not—federal insurance for banks. Now no bank would want to do without it," he adds. "Some companies are [giving prior notice of monitoring] right now and having no difficulties. I think it improves employee relationships," Simon says. In any case, he argues, "employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work." ■

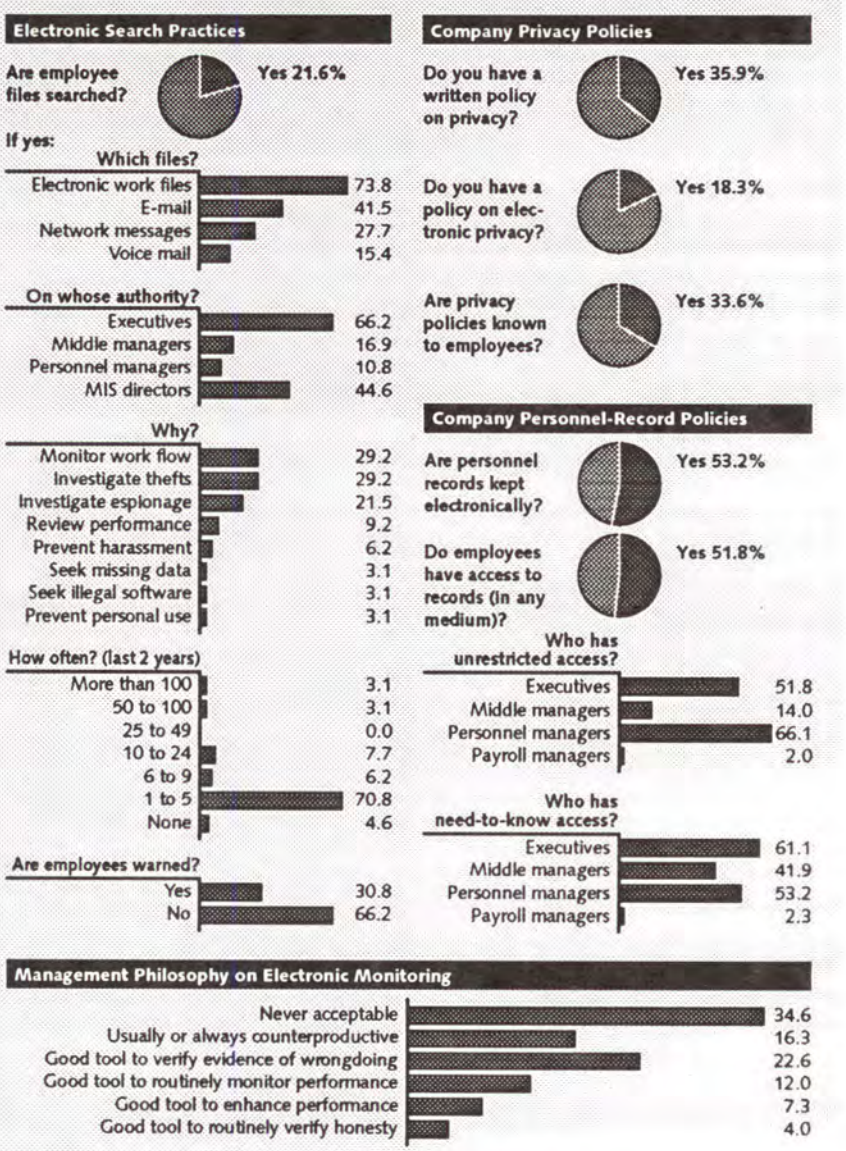
MACWORLD POLL

Electronic Eavesdropping at Work

Workers are routinely monitored in some industries, but how pervasive is the practice? To find out, *Macworld* conducted the first national survey designed to find out how and why businesses monitor employees. Top corporate managers from 301 businesses of all sizes and in a wide range of industries participated.

More than 21 percent of respondents—30 percent in large companies—have "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." Nearly 16 percent report having checked computerized employee work files, and 9 percent having searched employee E-mail.

These data suggest that some 20 million Americans are subject to electronic monitoring. Is your hard drive or office network searched? Better ask your boss directly. Only 18 percent of respondents' companies had a written policy regarding electronic privacy. And only 31 percent of companies that conduct electronic monitoring or searches of employee computers, voice mail, E-mail, or networking communications give employees advance warning.



Totals may not equal 100 percent, due to non-responses or multiple responses.
Margin of error for responses is ± 2.9 percent.

Research assistance by JIM CARR.

PRIVACY IN PERIL

How computers are making private life a thing of the past

BY CHARLES PILLER

In recent years, gathering and sharing personal information has become a way of life for business and government. People have kept track of one another for millennia, of course. But the advent of telecommunications, the growth of centralized government, and the rise of massive credit and insurance industries that manage vast computerized databases have turned the modest records of an insular society into a bazaar of data available to nearly anyone for a price.

The U.S. Constitution carries no explicit guarantee of personal privacy. But most Americans consider the ability to conduct one's personal affairs relatively free from unwanted intrusions to be an inherent human right. A year-long *Macworld* investigation shows that such a right stands little chance against new electronic technologies that make most people's lives as clear as glass.

From a personal computer anywhere in the world, data can be gathered from limitlessly broad and diverse sources. The ability to capture, sort, and analyze that data is often nearly instantaneous. The force of such tools has overwhelmed the capacity of laws and social mores to protect privacy.

Until the last few years, if you wanted to find out, say, if anyone had sued Roger Heinen, the former Apple vice president who defected to Microsoft in January, you had to laboriously check, in person, at various county courthouses. I spent about two minutes doing the same thing online.

"As technology becomes ever more penetrating and intrusive, it becomes possible to gather information with laserlike specificity and spongelike absorbency," says Gary T. Marx, a privacy expert who teaches at the University of Colorado. "Information leakage becomes rampant; indeed, it is hemorrhaging. Barriers and boundaries—be they distance, darkness, time, walls, windows, even skin—that have been fundamental to our conceptions of privacy, liberty, and individuality give way. Actions, feelings, thoughts, acts, even futures are increasingly visible." Easy access has blurred the borders of private life.

The public views these developments with growing alarm. In a 1992 poll conducted by Louis Harris and Associates, 78 percent of Americans expressed concern about their personal privacy, up from about a third of those polled in 1970, and up from 64 percent in 1978. Perceived threats to personal privacy from computers rose from 38 percent in 1974 to 68 percent last year.

In a 1991 *Time*/CNN poll, 93 percent of respondents asserted that companies that sell personal data should be required to ask permission from individuals in advance. The 1990 census showed the highest rates of noncooperation ever—the result of fears that participation could place personal information in jeopardy, contend some privacy advocates. And California's Privacy Rights Clearinghouse—the first privacy hotline in the nation—logged more than 5400 calls within three months of its inception last November.

What They Have on You

PUBLIC CONCERNS HAVE RISEN IN TANDEM WITH the proliferation of personal records kept by government, corporations, and employers. New forms of data are coming online all the time. Nearly every quantifiable aspect of our lives—and many a judgment call—finds its way into data banks where it is exchanged, sold, and resold, again and again.

The sheer volume of available data is stunning. In 1990, the U.S. General Accounting Office, an arm of Congress, conducted a survey of federal data banks that contain health, financial, Social Security, and a wide range of other personal data. That incomplete tally included 910 major data banks with billions of individual records. Much of the information

MICHELE CLEMENT

A Model Consumer-Privacy Code

Feeling the sting of consumer anger at the deluge of direct-marketing solicitations and credit-report problems, many companies have voluntarily established privacy codes of conduct. The following model code combines high points from corporate and trade-association policies with the views of privacy advocates. This model is based on reasonable expectations for business practices in today's world. Therefore, it does not address three ideas that could prove critical to protecting privacy in the long term:

- An opt-in system for direct marketing, in which the personal data would be collected only on consumers who request that their names be placed on marketing lists.
- Mandatory updates, audits, and correction of public records data.
- The option to replace *credit* cards that leave an electronic trail for every consumer transaction with anonymous *debit* cards, as some nations now do (see photo below). But for now, the following measures would go a long way toward protecting consumer privacy in electronic transactions.

Data Collection

- Fully disclose to consumers the nature of the data collected.
- Collect only data necessary to your business purpose.
- Contact consumers yearly to disclose current and anticipated secondary uses of their personal data, and to offer an opt-out option.

Direct Marketing

- For small companies: Don't sell detailed personal data that can be tracked to specific individuals. Do require customers to certify that list data will not be resold.
- For large companies: Don't sell personal data at all. Instead, charge customers to distribute marketing materials relevant to their interests.

Data Accuracy

- Conduct systematic and regular audits to catch data entry errors.
- Disclose the source of data on request from individual consumers.
- Provide easy and free methods for consumers to challenge records that concern them and if needed, to correct those records.

Data Security

- Limit access to personal data on a "need to know" basis—available only for legitimate business purposes.
- Train employees to prevent unauthorized disclosure, and audit their compliance at regular intervals.

Credit and Medical Data Bureaus

- Provide free yearly *complete* reports to consumers.
- Create a speedy appeal process for consumers to challenge their data.

Sunset Provisions

- Follow all laws in expunging incriminating records such as criminal convictions or bankruptcies.
- Periodically check for and purge all obsolete data.

Phone debit cards, such as this one from France, work like computer transit tickets. Each call's cost is deducted from the prepaid card, obviating detailed billing records.

from these computerized systems is open to other government agencies and corporations, or sold to thousands of commercial data banks that trade on records about your home, possessions, stock transactions, family characteristics, and buying habits.

And once created, a record rarely disappears. "In our society, there is a tendency to collect data without a clear purpose. And it stays around for years," says Alan Brill, head of the information-security practice for Kroll Associates, the largest and most successful private-investigation firm in the country. "It's like vampire data. It rises up from the dead to bite you," he says.

Obsolete information can mislead. Out of context, a single incriminating element in someone's personal history can become a defining characteristic. Suppose you were guilty of possessing a small quantity of marijuana in 1985, but haven't taken a toke since 1986. Should that conviction affect your employment prospects in 1993?

The problems grow when the data is wrong. If data banks contain millions or billions of records, it's hardly surprising that they sometimes slip a digit or two.

Consider the Big Three credit bureaus—TRW, Equifax, and Trans Union—which are among the largest and most closely monitored purveyors of personal data. These agencies compile and sell the records of key economic transactions for a large majority of American consumers.

Early this year, TRW agreed to pay $1000 each to about 1200 residents of Norwich, Vermont, whom the company erroneously designated as deadbeats due to a coding error. A 1988 survey of 1500 credit reports found that 43 percent contained errors. And a 1991 survey by Consumers Union found errors in 48 percent of reports requested from the Big Three, including 19 percent with inaccuracies that could cause a denial of credit, such as a delinquent debt. The Federal Trade Commission receives more complaints about credit bureaus than about any other industry.

Errors are not always the fault of the credit bureau—it might be from one of its sources. "In many cases the [credit bureaus'] responsibility to their customers is to give an accurate reflection of what's in the public record, and that public record may itself be inaccurate," explains Steve Metalitz, general counsel of the Information Industries Association, which represents about 500 companies that gather and resell data.

Regardless of the origin of such errors, there are no clear lines of responsibility for correcting the record. Meanwhile, the victim's life may descend into a Kafka-esque nightmare.

Values in Conflict

THE NEW STANDARDS OF ELECTRONIC intrusion upset the balance between two distinctly American values: an open and accountable society, and the right to be left alone.

There are many reasons to keep public records open and easily accessible. Society has the responsibility, for example, to monitor illegal activities, to capture criminals, and to preserve public safety. If electronic privacy rights were absolute, we would never have learned about Oliver North's E-mail messages, which helped unravel the Iran-Contra scandal. And organized-crime kingpin John Gotti might never have been convicted but for the tap on his phone.

Yet data collection has a dark side. In the 1960s and 1970s, J. Edgar Hoover's FBI gathered personal data by any means possible and often used it to blackmail innocent people, sometimes destroying their lives.

Employers have a right to guard against ineptitude, criminality, and cor-

Trade association spokesman Steve Metalitz: "In many cases, the [credit bureaus'] responsibility is to give an accurate reflection of what's in the public record, and that record may itself be inaccurate."

Privacy advocate Evan Hendricks: "To me, junk mail is not the most burning privacy issue, but I can see it annoys the hell out of a lot of people." He receives hundreds of letters that prove the point.

PHOTOGRAPHS BY MANUELLO PAGANELLI

Information industry lawyer Ronald Plesser: "Is the use of information compatible with the purpose for which it was collected?" If not, misinterpretation or crass exploitation usually follows.

porate spies. But should employers be free to search at will any and all employee computer files, E-mail, voice-mail, and data transmissions over a company's local area network? (See "Bosses with X-Ray Eyes," in this issue.)

Government investigators, members of the press, and the public at large may have a legitimate interest, for example, in knowing whether U.S. Transportation Secretary Federico Peña has ever been tagged for drunk driving. (We have no reason to believe he has.) But when the driving records of millions of people are sold to mass marketers of automobile insurance or alcohol-treatment programs, has the public trust been violated?

Beyond Junk Mail

THE ISSUE TRANSCENDS ELECTRONIC-list sales and the invasive micro-marketing tactics they stimulate. Personal data itself has become a commodity for sale on the open electronic market to anyone who owns a personal computer.

Take the case of Marketplace: Households, an ill-fated joint venture of Lotus Development Corporation, a software developer, and the Equifax credit bureau. Marketplace would have placed the names, estimated incomes, purchasing habits, marital status, and other data on 120 million consumers on a CD-ROM—the nation on a disc for only $700. Few consumers were persuaded by the project's privacy protections. And they let it be known: 30,000 angry letters killed Marketplace. Shortly thereafter, in the face of mounting consumer pressure, Equifax agreed to quit selling *any* consumer credit data to direct-marketing vendors.

In the space of a year Equifax went from promoting one of the most far-reaching incursions into privacy ever contemplated to opting out of the credit-data marketing business altogether. Early this year, TRW (but not Trans Union) followed suit.

But the personal-information market hardly depends on Equifax or TRW. Thousands of other data resellers—*Macworld* among them—offer lists of likely buyers. This wealth of sources has spawned a sprawling information-reselling industry. The Burwell Directory of Information Brokers describes 1253 commercial services with names like Disclosure, Access Information, and Answer Associates.

Many of those services provide only data on companies, economic trends, or sociopolitical issues. But personal information—address, marital, salary, driving, and employment history; corporate affiliations; who your neighbors are; vehicle and real estate holdings; civil and criminal court records—and much of the rest of the trail of bytes left by all of us is now available from scores of commercial sources. And to make their lives easier, the data-hungry turn to supermarkets of online information.

Down in the Data Mines

SO-CALLED SUPERBUREAUS BUY ACCESS to the major credit bureaus, state and federal agencies, and just about any other private or public-record repository they can find. They provide one-stop shopping for online data. The data-reselling trade is the electronic equivalent of the gold rush—few legal restrictions apply, and there is lots of money to be made if you own the mine.

Standards vary widely, but some information brokers are less than scrupulous in screening their clients. Even legally shielded data, such as credit and phone records, as well as arrests that do not result in convictions, frequently are revealed to a wide range of qualified or merely determined and savvy requesters. These include private investigators, direct marketers, the press, FBI agents, lawyers, insurance companies, corporate spies, and vindictive ex-spouses.

The U.S. is a laughingstock among privacy experts because we protect video-tape-rental records, but not medical records

For data mining to be worthwhile, the information has to be difficult or impractical to obtain using conventional methods, but worth the cost of electronic extraction. It is.

Consider the results of an online experiment my colleague Galen Gruman and I conducted during research for this article. First we selected prominent individuals from the entertainment industry,

Shattering the Illusion of Privacy

THE GOAL

How easy is it to obtain someone's home address? Social Security number? Real estate holdings? *Macworld* investigated 18 business leaders, politicians, Hollywood celebrities, and sports figures. We primarily targeted residents of California, where most public records are online, and sought all legally accessible data available from four commercial and two governmental data suppliers. We exhausted the systems' resources after spending about $112 per subject. In addition to the records shown below, we searched public records for criminal court filings; fictitious business names; and records of bankruptcies, insider trading transactions, trusts, deeds, powers of attorney, and other legal matters.

THE SUBJECTS

In addition to the pictured subjects, we obtained similar data on U.S. Attorney General Janet Reno, U.S. Representative Robert K. Doman, actor Clint Eastwood, Microsoft executive Roger Heinen, former U.S. Attorney General Edwin Meese III, restaurateur Wolfgang Puck, San Francisco Mayor Frank Jordan, and several others.

	George Lucas Movie producer	Joe Montana Football star	Leon Panetta Director, U.S. Office of Management/Budget	William R. Hearst III Publisher, *San Francisco Examiner*	Richard M. Rosenberg CEO, Bank of America
WHAT WE FOUND					
Personal Data					
Birth date	✓		✓	✓	✓
Home address	✓	✓	✓	✓	✓
Home phone	✓		✓		✓
Social Security number	✓		✓	✓	✓
Neighbors' address/phone	✓	✓	✓	✓	✓
Driver record*	✓		✓	✓	✓
Marriage record	✓	✓	✓	✓	
Voter registration				✓	✓
Biography	✓		✓	✓	✓
Legal/Financial Data					
Tax liens	✓			✓	
Campaign contributions**	✓		✓		✓
Vehicles owned			✓	✓	✓
Real estate owned	✓	✓	✓	✓	✓
Commercial loans/debts	✓	✓		✓	
Civil court filings	✓	✓	✓	✓	✓
Corporate ties***	✓	✓		✓	✓

FROM LEFT TO RIGHT: GREG GORMAN/GAMMA LIAISON; ADAM SCULLICOMBE PHOTOS; BRAD MARKEL/GAMMA LIAISON; WILL MCCROVE; ED KASHI

*Includes physical characteristics. **$200 or greater contributions, federal offices only. ***CEO or registered agent of a corporation.
Macworld does not guarantee the completeness or accuracy of the records we obtained.

business, politics, the Macintosh industry, and sports, including Hollywood producer (and friend of President Bill Clinton) Harry Thomason, former San Francisco 49ers quarterback Joe Montana, and Bank of America CEO Richard Rosenberg. Then we tried to find out everything we could on them, with the following restrictions: we did not seek legally protected data, and all the information had to be obtained online.

For this modest search we spent an average of only $112 and 75 minutes per subject. Even so, we unearthed the essential financial, legal, marital, and residential histories of nearly all of our subjects (see the chart "Shattering the Illusion of Privacy"). In short, we compiled electronic dossiers. And these were the efforts of data-mining neophytes.

As online services become increasingly interconnected, affordable, and fast, the ability to build electronic dossiers may quickly become the hottest privacy issue of the next century. Then again, there are so many pressing privacy issues and such widely divergent sensibilities about personal privacy, even professional privacy advocates have trouble deciding what's most important.

A Question of Priorities

"TO ME, JUNK MAIL IS NOT THE MOST burning privacy issue," says Evan Hendricks, editor of the *Privacy Times* newsletter. "But I can see it annoys the hell out of a lot of people." To illustrate the point, he pulled out a box of 300 recent letters from consumers apoplectic over a deluge of unwanted letters flowing into their mailboxes. Financial interests and personal sensibilities about electronic privacy cover an enormously broad spectrum. This makes it hard to separate trivial problems from real invasions that damage people.

"You have to choose a certain bundle of records, prioritize those records, and create a trustee situation around them," argues Jerry Berman, Washington, D.C., director of the Electronic Frontier Foundation, an advocacy group for computer users. "You cannot protect all data, bit by bit, byte by byte."

What should be in the bundle? Medical records are a top priority "due to the sensitivity of the data and the lack of any existing legislation to protect it," says Ronald Plesser, a lawyer who represents the information industry and headed President Clinton's transition team for the Federal Communications Commission. Tighter privacy controls for banking, tax, and credit records are also near the top of every privacy advocate's list.

"Around the world, the U.S. is a laughingstock among privacy experts because we have a law protecting videotape-rental records, but not medical records," Hendricks adds. (The release of individual video-rental records was sharply restricted after a reporter finagled the details of Judge Robert Bork's viewing habits during his confirmation hearings for a seat on the U.S. Supreme Court two years ago.)

Outcry over Credit Records

PUBLIC OUTCRY AND POLITICAL PRESsure have already reformed the major credit bureaus: all three bureaus now permit consumers to view and correct credit reports, although the reports released to consumers may not be as detailed as those given to, say, prospective employers or landlords. What's missing is usually information like an assessment of the person's credit risk.

TRW makes reports available free to individual consumers. Equifax has opened a toll-free line (800/685-1111) to respond to consumer questions. Bad publicity has prompted credit agencies—particularly Equifax—to more strictly screen companies and information brokers who seek access to credit reports. And in February, federal legislation was introduced that would force credit bureaus to correct errors within 30 days, and would hold banks and retailers accountable for the quality of the information they turn over to credit bureaus.

But credit records represent only a small fraction of online personal data. The far broader category of public-records data—real estate ownership, court records, tax liens, bankruptcy filings, voter registration data, auto and driver records, marriage records, and the like—should be on the table, argues Jan-Lori Goldman of the American Civil Liberties Union's Privacy Project.

"We're now asking a question that hasn't been asked before: What is the public's interest in accessing this information?" she says. Should the price of a driver's license be that you give up your detailed personal description to anyone who wants to buy it? Privacy advocates call for a close look at online data mining and they recommend limits on the collection of unduly detailed electronic dossiers.

Plesser, the Clinton transition team adviser, suggests using this test: "Is the use of the information compatible with the purpose for which it was collected?" When the answer is no, the prospect of misinterpretation or crass exploitation usually follows.

Do Access and Privacy Conflict?

MANY LAWYERS, DIRECT MARKETERS, and reporters say that radical restrictions on public-records data would give them electronic migraines, and could even make their jobs impossible. But Marc Rotenberg, Washington, D.C., director of Computer Professionals for Social Responsibility, warns against believing arguments that access and privacy rights are inherently incompatible. Such conflicts are often promoted by those who stand to profit by expanding access to private data, he argues.

Take the case of caller ID. Such systems instantly reveal a caller's number on a display attached to the phone of the party receiving the call. Caller ID has often been portrayed in the media as a simple case of competing consumer interests—some people advocate the system as a way to apprehend heavy breathers; others fear caller ID as an open invitation for businesses to surreptitiously pad marketing lists and for bullies to find battered spouses hiding in shelters.

But there is a third factor. "With the advent of caller ID, the telephone companies stood at the fulcrum of this information transfer and stood to benefit from the proposed sale of personal telephone numbers," Rotenberg says. How? They can charge businesses for using the caller ID service and then charge consumers for being listed or not listed, depending on the local laws' requirements.

Managing Electronic Privacy

HOW SHOULD SUCH CONFLICTS BE resolved? In the U.S., a wide range of federal and state agencies grapple with privacy issues. Sometimes they have exemplary tools to work with, such as the Electronic Communications Privacy Act, which bans most electronic eavesdropping over phone or data lines.

More often, there is little or no legal protection of personal data. Part of the reason may be that no government agency reviews privacy issues comprehensively or tries to map a coherent overall policy on the wide range of consumer, commercial, and workplace privacy issues.

Canada and many European nations use privacy commissions or data-protection agencies to advise their governments on privacy policy, protect consumer rights, or regulate corporations. Most privacy advocates in this country see some kind of privacy board—staffed with specialists equipped to evaluate emerging privacy issues—as a key to timely and effective regulation.

Our society collects and stores data without a clear purpose. It's like vampire data. It rises up from the dead to bite you.

"The U.S. is an embarrassment to the privacy movement overseas," says Simon Davies, director of the Australian Privacy Foundation. "The U.S. stands alone as an example of what a superpower should not do in privacy."

A U.S. data-protection board with advisory powers was proposed in Congress in 1991. Proponents believe that such a board could sort out the privacy implications of new services or technologies before they saturate the marketplace or are unnecessarily quashed by consumer outrage.

The developers of Lotus Marketplace might have averted years of fruitless development if a privacy board had offered feedback on the idea in advance. The National Research and Education Network (NREN), promoted by the Clinton administration, would be a prime candidate for advance evaluation by a privacy board. This multibillion-dollar "data superhighway" would theoretically allow tens of millions of Americans to communicate data, voice, video, and other forms of media at many times the speed of current networks. Protecting personal information on NREN is "*the* privacy issue of the twenty-first century," says the Elec-

11 Easy Ways to Safeguard Your Electronic Privacy

Other than a few hermits living on remote mountain peaks, few of us can realistically give up insurance, credit cards, and electronic banking. Sacrificing some personal privacy is the price of admission to our consumer society. But the following steps can curb some of the worst invasions of privacy in the lives of today's consumers.

Personal Identification

- Give only the minimum data required for commercial transactions. Leave all Social Security, home phone, driver's license, and credit card numbers off checks whenever possible. And don't give such numbers for credit card purchases; in most cases they are not needed by merchants.

Credit

- Obtain your credit report yearly from one or more of the big three credit bureaus (Equifax, Trans Union, and TRW; to contact these companies check for an office in your area), and try to correct any errors you detect.
- When rejected for credit, ask why; then verify the accuracy of the data used to reject you.

MANUELLO PACANELLI

Charles Hamel, a critic of the Alyeska Pipeline Service Company, which operates the trans-Alaska oil pipeline, was the subject of an elaborate spying operation initiated by the company. Alyeska, through a third-party investigator, gained access to Hamel's credit and phone records, as well as personal financial data.

Insurance

- Obtain a free copy of your medical record from the Medical Information Bureau (617/426-3660), an agency used by more than 750 insurance companies to calculate financial risk. If (in consultation with your doctor) you detect errors, contact the bureau and demand that the record be corrected promptly.
- When rejected for insurance, ask why; then verify the accuracy of the data used to reject your policy application.

Marketing

- When offered "free" premiums, rebates, or other incentives in return for giving personal data for a marketing list, find out who will use the data and for what purpose. Ask if you can participate by giving minimal information, such as name and address.
- When you return warranty cards, provide only information essential to the warranty service. Ignore personal questions used only for marketing.
- To pare back junk mail, calls, and faxes, check the "opt-out" box many companies offer on warranty forms and subscription cards. Ask solicitors to take your name off their lists, and get the Direct Marketing Association (212/689-4977, ext. 369) to remove your name from its members' lists.
- If you participate in marketing or public opinion surveys, verify that answers will be used only in conjunction with those of other respondents, and that no personal information can be traced back to you.

Telecommunications

- Some states allow caller ID services—a way to view a caller's phone number on a monitor attached to your phone before answering. In most such states, the phone company must provide callers with an option to block viewing of their number. Ask your phone company to set up that blocking ability.

Banking

- Ask your bank to agree in writing to disclose your personal financial records only to legally authorized requesters, and to notify you when such requests are granted.

tronic Frontier Foundation's Berman, yet so far the government has ignored the privacy implications of the project.

With powerful industry interests arrayed against it, privacy-board legislation has gone nowhere. "American consumers have more choice than any other consumers in the world. Part of the reason is that we are an open information society," says Lorna Christi of the Direct Marketing Association, echoing the industry's general fear of government regulation. "Self-regulation is working."

John Baker, senior vice president of Equifax, supports the idea of a board that conducts research and gives confidential advice to industry. But he objects to giving a privacy board the very investigative and complaint-resolution responsibilities that privacy advocates see as minimum requirements to safeguard consumer and worker rights.

For now at least, the privacy implications of new technologies are likely to be confronted by government on an ad hoc basis, and only after the public has cried out for relief.

The Role of Technology

PRIVACY ADVOCATES ARE FOND OF SAYing that the United States is "first in technology, last in privacy protection." And while technology has made our personal lives more transparent, privacy and technology are not inherently antagonistic. In the absence of a privacy board, new technologies may prove one of the most potent forces driving what *Privacy Times*'s Hendricks calls "the right to informational self-determination."

Technology has already alleviated many everyday intrusions: Airport X-ray units have made hand searches of luggage rare. With magnetic markers in books and clothing, searches of purses or briefcases in libraries and stores are quickly becoming obsolete. And encryption software makes computer files infinitely more secure than paper documents in locked cabinets.

A California company has even developed a "video game" to replace drug testing for truck drivers and other workers. Before each shift, employees go through a short hand-eye coordination exercise at a computer terminal. If they fail this simple test, they skip the shift or are moved to less demanding work that day. The technique not only screens out drug or alcohol intoxication, but also seems to identify workers who are excessively fatigued or preoccupied. One trucking company reports a dramatic decrease in accidents and worker errors after a year using the system.

Such stories are encouraging, but so far they are rare. Industry and society face a daunting challenge: to develop technologies that protect personal privacy faster than those that threaten privacy.

The stakes are high. "Privacy allows us to move freely between the public world and private world, to form smaller communities within the larger community, to share our concerns, dreams, and beliefs with our close friends. To have secrets," Rotenberg commented in an online forum sponsored last year by the *Wall Street Journal*. "There is a close tie between privacy and pluralism. . . . This is what I suspect is at risk in the current rush to record and exchange personal data. Global Village in theory. Surveillance State in practice." ■

MACWORLD POLL

Electronic Eavesdropping at Work

Workers are routinely monitored in some industries, but how pervasive is the practice? To find out, *Macworld* conducted the first national survey designed to find out how and why businesses monitor employees. Top corporate managers from 301 businesses of all sizes and in a wide range of industries participated.

More than 21 percent of respondents—30 percent in large companies—have "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." Nearly 16 percent report having checked computerized employee work files, and 9 percent having searched employee E-mail.

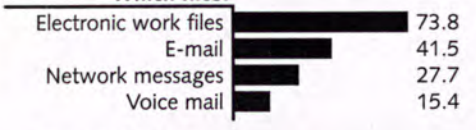
These data suggest that some 20 million Americans are subject to electronic monitoring. Is your hard drive or office network searched? Better ask your boss directly. Only 18 percent of respondents' companies had a written policy regarding electronic privacy. And only 31 percent of companies that conduct electronic monitoring or searches of employee computers, voice mail, E-mail, or networking communications give employees advance warning.

Electronic Search Practices

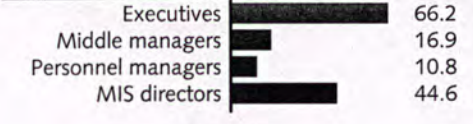
Are employee files searched? Yes 21.6%

If yes:

Which files?

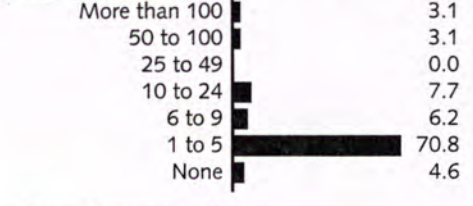


On whose authority?

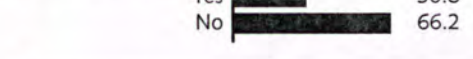


Why?

How often? (last 2 years)



Are employees warned?



Company Privacy Policies

Do you have a written policy on privacy? Yes 35.9%

Do you have a policy on electronic privacy? Yes 18.3%

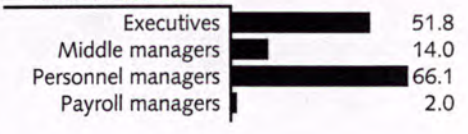
Are privacy policies known to employees? Yes 33.6%

Company Personnel-Record Policies

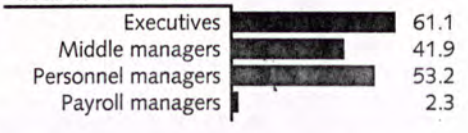
Are personnel records kept electronically? Yes 53.2%

Do employees have access to records (in any medium)? Yes 51.8%

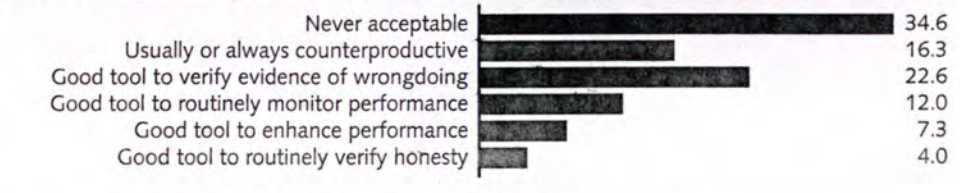
Who has unrestricted access?



Who has need-to-know access?



Management Philosophy on Electronic Monitoring



Totals may not equal 100 percent, due to non-responses or multiple responses.
Margin of error for responses is ± 2.9 percent.

Shattering the Illusion of Privacy

THE GOAL

How easy is it to obtain someone's home address? Social Security number? Real estate holdings? *Macworld* investigated 18 business leaders, politicians, Hollywood celebrities, and sports figures. We primarily targeted residents of California, where most public records are online, and sought all legally accessible data available from four commercial and two governmental data suppliers. We exhausted the systems' resources after spending about $112 per subject. In addition to the records shown below, we searched public records for criminal court filings; fictitious business names; and records of bankruptcies, insider trading transactions, trusts, deeds, powers of attorney, and other legal matters.

THE SUBJECTS

In addition to the pictured subjects, we obtained similar data on U.S. Attorney General Janet Reno, U.S. Representative Robert K. Dornan, actor Clint Eastwood, Microsoft executive Roger Heinen, former U.S. Attorney General Edwin Meese III, restaurateur Wolfgang Puck, San Francisco Mayor Frank Jordan, and several others.

FROM LEFT TO RIGHT: GREG GORMAN/GAMMA LIAISON; ADAM SCULL/GLOBE PHOTOS; BRAD MARKEL/GAMMA LIAISON; WILL MOSGROVE; ED KASHI

WHAT WE FOUND

	George Lucas Movie producer	Joe Montana Football star	Leon Panetta Director, U.S. Office of Management/Budget	William R. Hearst III Publisher, *San Francisco Examiner*	Richard M. Rosenberg CEO, Bank of America
Personal Data					
Birth date	✓		✓	✓	✓
Home address	✓	✓	✓	✓	✓
Home phone	✓		✓		✓
Social Security number	✓		✓	✓	✓
Neighbors' address/phone	✓	✓	✓	✓	✓
Driver record*	✓		✓	✓	✓
Marriage record	✓	✓	✓	✓	
Voter registration				✓	✓
Biography	✓		✓	✓	✓
Legal/Financial Data					
Tax liens	✓			✓	
Campaign contributions**	✓		✓		✓
Vehicles owned			✓	✓	✓
Real estate owned	✓	✓	✓	✓	✓
Commercial loans/debts	✓	✓		✓	
Civil court filings	✓	✓	✓	✓	✓
Corporate ties***	✓	✓		✓	✓

**Includes physical characteristics. **$200 or greater contributions, federal offices only. ***CEO or registered agent of a corporation.*
Macworld does not guarantee the completeness or accuracy of the records we obtained.