

MEMORANDUM

TO: BRUCE REED, ELENA KAGAN

FROM: TOM FREEDMAN
MARY SMITH
JULIE MIKUTA

RE: INFORMATION PRIVACY

DATE: JULY 14, 1997

SUMMARY

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

I. CONSUMER PRIVACY SURVEY

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

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

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

II. TASK FORCE REPORTS UNDER THIS ADMINISTRATION

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

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

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

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

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

1. The Secretary of Commerce and the Director of the OMB will encourage private industry and privacy advocacy groups to develop and adopt effective rules to protect privacy on the Internet. These rules will be consistent with the Privacy Principles.
2. The Secretary of Commerce will encourage private industry to develop and adopt a filtering device that will enable Internet users to screen content not suitable for children.
3. All agencies and departments will promote efforts to make the Internet secure for e-commerce.

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

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

Recommendations for improving data protection policies

The report recommends these strategies to improve privacy protection:

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

2. The government could ensure that government data collection remains consistent with the Privacy Principles in the face of changing technology. The OMB's Office of Information and Regulatory Affairs has statutory responsibility with respect to the privacy legislation and could review these statutes in light of the Privacy Principles as a model for audits in the private sector. Recently, the HHS and IRS have established Privacy Advocates; this practice could be expanded to all agencies.
3. The government could play a larger role in consumer and business education. Agencies could act as "bully pulpits" to raise consumer and business awareness of this issue.
4. Government could enhance self-regulation by exploring U.S. competition law that is blamed for enforcement deficiencies with industry.
5. A federal entity with regulatory authority could be created that would drive the development of Federal data privacy policy, or oversee the various initiatives now underway.
6. A federal body without regulatory authority could be created that would: coordinate privacy policy; represent the President's views both domestically and internationally; advocate the use of fair information practices by governments and the private sector; play an advisory role in the public and/or private sector; educate consumers and businesses about privacy; involve itself in the litigation of certain cases where a citizen's or group's privacy has been unfairly invaded. The faxed Memorandum states that the Privacy Options Paper suggested the OCA could serve this function; this does not appear to be the case.
7. A non-governmental or advisory body could be created that would perform an advisory function in the public and/ or private sector.

The Privacy Principles

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

1. ***General Principles:*** Personal information should be acquired, disclosed and used only in ways that respect an individual's privacy. It should not be altered or destroyed, and should be accurate and relevant for the purpose for which it is provided and used.
2. ***Principles for Users of Information:*** Information users should assess the impact on privacy in deciding whether or not to acquire, disclose or use personal information. They should inform individuals about whom the information is being collected about why they are collecting the data, what it will be used for, how it will be handled; the consequences of providing or withholding information; and any rights of redress.

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

III. THE OFFICE OF CONSUMER AFFAIRS' PRIVACY PROTECTION PRINCIPLES

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

1. Tell consumers, in easily understood language, when and why certain information is being collected, what's going to be done with it, and who will have access to it. Tell them how you plan to protect their privacy, and ask for feedback.
2. Collect only information applicable to the transaction at hand. Do not allow the information to be used or sold for other incompatible purposes without the individual's knowledge.
3. Provide consumers a copy of their files upon request, and make it easy for them to correct errors and use statements of explanation.
4. Allow consumers to opt in to direct marketing or other uses they feel are appropriate for the information they are providing.
5. Make a concerted effort to educate consumers generally about how information about them is gathered, analyzed, grouped into lists and rented or sold, or otherwise used.

IV. THE EUROPEAN COMMISSION

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

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