

FOIA MARKER

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

Collection/Record Group: Clinton Presidential Records
Subgroup/Office of Origin: Council of Economic Advisers
Series/Staff Member: Timothy Brennan
Subseries:

OA/ID Number: 24354
FolderID:

Folder Title:
Privacy IITF [Information Infrastructure Task Force]

Stack:	Row:	Section:	Shelf:	Position:
S	21	3	6	2

EXECUTIVE OFFICE OF THE PRESIDENT
COUNCIL OF ECONOMIC ADVISERS
WASHINGTON, D.C. 20502

TIMOTHY J. BRENNAN
SENIOR ECONOMIST

PHONE: 202-395-5614
FAX: 202-395-6809

To: Gerald Gates, Policy Office
Bureau of the Census

Cc: Sally Katzen, Administrator, OIRA, OMB
Joseph Stiglitz, Chair, CEA
Michele Jolin, Chief of Staff, CEA

From: Tim Brennan¹ 
Senior Economist, CEA

Date: Aug. 27, 1997

Re: IITF Privacy Working Group Draft Report

The IITF Privacy Working Group Draft Report is a thoughtful and thorough description of the current state of the law regarding privacy and the potential consequences that new information technology will have on the ability of individuals to control the distribution of information about themselves. Readers who are not already expert in this complex legal and policy area, such as myself, will learn a great deal about their vulnerability and the absence of systematic constitutional rights or statutory protections of their privacy interests. While the law may provide some uniform guarantees regarding the government's acquisition and use of personal information, there is apparently much less protection regarding the distribution of personal information acquired by private corporations and other entities regarding medical histories, financial transactions, and to some extent data supplied to the government and subsequently sold by it to private parties.

Following internal review, this Report will be published in the Federal Register to solicit comment from the public. At this stage in the process, the most useful comments to make would have to do with factual errors. Again, not being a thorough expert in the laws relating to privacy, I have nothing to say on those questions. I do have a few suggestions regarding general principles and approaches, but it may make more sense for the Working Group for consideration as they consider the broad range of comments that the public is sure to offer on this timely and important document.

¹ This memo represents my opinions and does not necessarily reflect those of the CEA.

1) What should the limits on privacy be? Perhaps I'm reflecting my academic disposition, but one difficulty I had in processing the vast amount of information contained in the Report was that it offered no clear framework for deciding when public or private use and dissemination of personal information was improper. For example, following the lead of the IITF's Intellectual Property Task Force Report, why not treat personal information as if it were copyrighted, and that every electronic display of that information is an infringement on the persons rights? When if ever should someone be permitted to distribute information about a person without that person's consent? If not, can we describe principles for explaining when there should be exceptions to that rule?

A phrase that brought this conundrum most vividly to mind is on p. 3, where the Report says

Thus, the crucial question becomes: how do we balance the need to use information (by government, commerce, and individuals) with the right of individuals to decide what information about themselves will be exposed to others?

Consider the following very similar statement:

Thus, the crucial question becomes: how do we balance the need to use labor (by government, commerce, and individuals) with the right of individuals to decide how their labor will be used by others?

We have a simple way of deciding the second question: We give individuals virtually absolute property rights in their labor. If uses of a person's labor are more valuable to government, business, and other individuals than that time and effort are worth to that person, the former can offer the latter a wage or salary in excess of that worth. Market exchange ensures that the "crucial ... balance" is met: a person supplies labor only when its value to others exceed his or her most valuable alternative occupation (including leisure, raising a family, pursuing non-work related interests).

Why should we not apply this "labor" principle to personal information? Among the possible reasons are:

- Persons have monopolies over information about themselves and may not want to give it up except at an excessive price.
- Unlike intellectual property, private information costs nothing to "produce" and thus we don't need to give people financial incentives to produce it.
- Markets are known to fail to work when participants on one side of a market know something about themselves (e.g., private health risks) that those on the other side (e.g., insurers) do not know.
- Perhaps there are cases in which the benefits to a private buyer of information about a person are less than those generated to society as a whole, because of

some “external” effect, e.g., knowing that someone with a driver’s license is near-sighted and shouldn’t drive without eyeglasses.

- In some cases the cost to the individual from giving up information about himself or herself is the result of activity that imposes costs on society as a whole--e.g., crime--and thus to let criminal suspects set the price for revealing information about themselves would destroy the deterrence effect of criminal punishments.

Except perhaps for the first and last of these, all of these arguments are problematic. I have a hard time coming up with plausible examples for the “asymmetric information” and “externality” cases that would rationalize stripping the right of an individual to control information about himself or herself. But fine design of new laws and institutions to manage privacy depends in part on our ability to define circumstances in which privacy rights *should* be abrogated, and how making information electronically available may change those standards. If there are no such circumstances, do we need any new policy or institutions beyond granting people a “copyright” in personal information?

2) Constitutional standards. An important constitutional standard, at least in asserting privacy rights against the government, is whether a person has a “reasonable expectation of privacy” *vis a vis* the nature of the information. In the electronic world, this standard may say little as a factual matter, since the “reasonable expectation” is itself a product of legal and political decisions. For example, if the government were to pass a law saying that all email was accessible to the government under any circumstance, no one could then claim to have a “reasonable expectation of privacy” regarding email. If, on the other hand, a “reasonable expectation” describes how much privacy a person *should* have, instead of what he or she believes he *does* have, we need to be more precise about the principles defining limits, if any, to privacy rights.

3) How does the common law fit in? The Report’s discussion centers on statutes relating to areas of federal records, communications, medical histories, and commercial transactions. The discussion of constitutional protections is brief, since the concern in the article is on nongovernment use and electronic distribution of personal information. It might be worth mentioning what if any protections are afforded individuals through common law litigation, e.g., treating invasion of privacy as a tort. Limits of the common law *in fact* could provide some insight into the limits of privacy rights *in principle*.

4) Another technology. This is blowing my own little horn a bit, but prior to coming to the CEA, I did some research with Dr. Molly Macauley, a space economics expert at Resources for the Future, on remote sensing satellites and their consequences for privacy.² Improvement in the technology of imaging, communication, and desktop data processing could give make public detailed locational information in ways that persons could do little if anything about. (These technologies are likely have consequence for industrial competition and international relations as well.) For whatever it’s worth, this is not merely a sub-

² T. Brennan and M. Macauley, “Remote Sensing Satellites and Privacy: a framework for policy assessment,” *Law, Computers, and Artificial Intelligence* 4 (1995): 233–48.

ject for academic speculation; I've attached a copy of a recent article from *The Atlantic* discussing remote sensing.

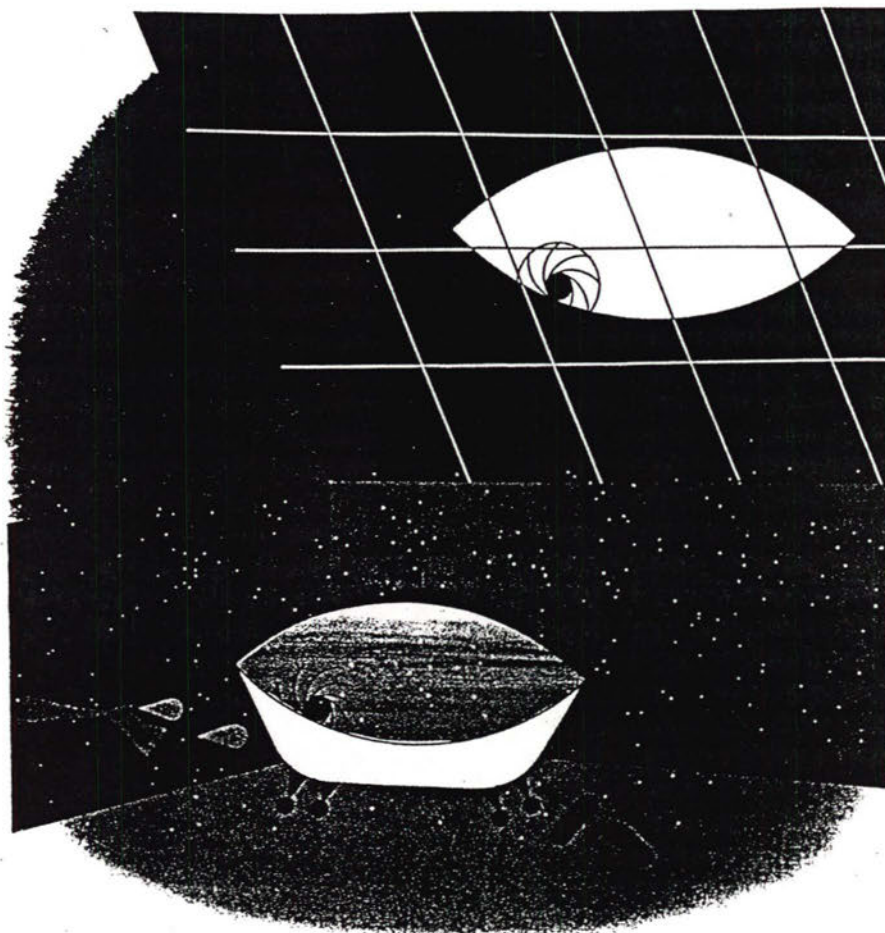
5) Market solutions. The Report deserves many accolades for acknowledging the possibility that markets in both legal contracts and technical devices may arise to provide privacy to those consumers who value it the most. Whether those seeking privacy or those who want information about them should pay may not be an important policy question, if those markets would work well either way. That, however, remains to be seen.

Along these lines, encryption technology has been the subject of a great deal of policy discussion both in the executive branch and, I believe, in Congress as well. Nothing in this Report even alludes to this controversy.

6) Institutional alternatives. The Report concludes by comparing

- the *status quo* of *ad hoc* public actions and marketplace reactions to privacy concerns,
- an “enhanced government” role that would include enacting new statutes, facilitating markets in privacy enhancing institutions and products, and using the “bully pulpit,” and
- the obvious favorite, a new federal privacy policy coordinating institution placed either on a large scale in an executive department or a new independent regulatory commission, or on a small scale as an executive agency “spokesperson” or advisory committee.

The choice among these different institutional alternatives may require not just a sense that we have a *big* problem, which the Report conveys quite well, but what exactly *makes* the problem so big? Understanding the limits of privacy protection, and the limits of its common law protection as well as the patchwork of statutes and constitutional doctrines, could help the readers understand better just why we might need a new agency, and what its most important roles might be.



High Resolution, Unresolved

Private companies will soon launch satellites powerful enough to spot environmental hazards—or a car in your driveway. Should we worry about snooping from space?

FOR more than thirty years spy satellites launched by the United States have been gathering a "virtual time-machine record of the earth," as Vice President Al Gore has described it. The public has paid close to \$100 billion for that record. But national-security and personal-privacy concerns

by **Mary Graham**

have blocked the use of the world's most powerful sensors to make current information about natural resources, environmental hazards, and private property in the United States available to environmental scientists, government agencies, and businesses. Because the Central Intelligence Agency is barred by

federal law from spying on Americans, it shares current environmental information about the United States only in rare instances—for example, in response to natural disasters.

Now, though, spy-satellite technology that has been used for a single purpose—espionage—with extraordinary government controls can suddenly be used for any purpose with few controls. In 1994, concerned about the post-Cold War health of the U.S. aerospace industry and fearful that foreign competition might challenge U.S. leadership in satellite technology, the Clinton Administration decided that private companies could launch satellites with high-resolution sensors previously available only to the intelligence community, and could provide information to anyone willing to pay for it. As government officials take cautious steps to share information gathered by military satellites, four U.S. companies are racing to launch satellites of their own equipped with similar technology. The first launch is scheduled for later this summer.

At a recent conference in Washington, D.C., Mark Brender, ABC's Pentagon producer, predicted that precise pictures from space will revolutionize television news, both by freeing reporters from relying on government-provided information during international crises and by freeing viewers from relying solely on what reporters tell them. David Bohrmann, an executive producer at NBC, demonstrated how networks could use satellite pictures to simulate flyovers of troop encampments in Bosnia. At his command a technician in New York using prerecorded images zoomed in on villages, scanned rivers, and hovered over military bases, producing a moving picture that resembled a helicopter ride around the countryside.

WHAT is really at stake is the ground rules for the next phase of mapping the earth. By next year three of the four companies plan to produce images of one-meter resolution—100 times as precise as those of current civilian satellites. The ability to see hazy outlines of large buildings will be replaced with the ability to see the clear shapes of small

cars. The ability to observe the same farm or city block every sixteen days will be replaced with the ability to observe the same point every two or three days; three to six images a day of most places in the United States are promised within four years.

Fundamental issues are being decided now. When should the government be allowed to censor images to protect national security? Should fears of military snooping from space be replaced with fears of snooping by corporations or domestic agencies? Will access to satellites' most detailed pictures pass from a small cadre of military clients with top-secret clearance to a small cadre of corporate clients with the means to pay for them?

Since commercial use of this technology is new, no one has a ready framework for resolving questions about national security, the protection of privacy, and public access to information. Time-tested principles that allow the government to block information in emergencies, keep homes and their surroundings free from intrusion, and treat geographic information as a national resource can provide guidance—if they are heeded. The breadth of the government's power to censor images may be decided this fall, when the Commerce Department is expected to issue final policies setting the conditions for commercial licenses to operate satellites. Privacy questions may be decided in an international context: strict privacy rules adopted by the European Union last July require consent for the use of information that identifies an individual. They may keep companies in the United States from selling images abroad unless similar rules are approved in this country. Access questions—whether images can be copied and distributed to the public, for example—will probably be negotiated between satellite companies and their customers, including government agencies.

NO longer simply the source of spectacular views of the earth, satellite images have a new capacity to influence what people do and how they think. Using sophisticated software and powerful, inexpensive computers, businesses, government agencies, citizens, groups, and individuals can now produce layered

maps (called Geographic Information Systems, or GIS) that combine new environmental findings with information already available to the public, such as property ownership and census data. New satellites will make such maps more useful by providing high-resolution images with digital precision and offering predictable repeat visits. Neither aerial photography nor current civilian satellites like Landsat or the French SPOT can produce this combination.

The investigative powers of satellites derive not just from photography but from sensors measuring visible and invisible wavelengths of the sun's energy. These can reveal more about an object's character than can be discovered standing next to it: each species of plant, type of soil, and kind of rock or building material, for example, uniquely reflects and absorbs wavelengths. Experts add a few caveats: measures of reliability are critical; interpretation is complicated; and much of this science is still in its infancy. And like all maps, these reflect the quality of underlying information.

Information from sensors can give early warning of environmental hazards. Kass Green, the president of Pacific Meridian Resources, a mapping firm, expects that new images will help minimize the damage done by wildfires like those that sweep through urban areas such as Los Angeles and Oakland, California. For the first time, she says, it will be possible to easily distinguish asphalt, wood-shake, and synthetic-shake roofs and to assess from week to week the dryness of vegetation around homes. Planning firebreaks and other preventive measures depends on accurately predicting a fire's path.

Satellite maps can help to settle political controversies—or create them. When, for example, environmental groups and the Bush Administration clashed over how much old-growth forest in the Pacific Northwest should be protected as habitat for the spotted owl, competing layered maps produced by the Wilderness Society and the federal Forest Service provided a basis for negotiation, by clarifying different ways of defining old growth. New maps of Latin America that were completed last fall by the World Wildlife Fund have led to a debate about how to use limited conservation funds: the maps make

clear that tropical dry forests and grasslands are as important to biodiversity as rain forests, and are more severely threatened.

Satellite images can make things harder to hide. The Environmental Protection Agency has used such images to help identify hazardous-waste sites and sources of water pollution. European farmers, who receive crop subsidies of \$50 billion a year, have new reasons to submit accurate information: their planting patterns are monitored from space by the European Commission. When farm boundaries are layered over images of the countryside, infrared color codes reveal whether a field is growing barley, wheat, corn, or something else.

OF course, newly explicit images can also be used to make mischief. Foreign intelligence agencies are expected to be among the largest buyers of high-resolution images. "International security issues are serious," says Ray Williamson, a senior research scientist at the George Washington University Space Policy Institute. "Iraq would be interested in information about Saudi Arabia. Iran would like to see data about Israel. India and Pakistan would like to have information about each other. If you were concerned about troop buildup on your border, you could put in a standing order for the satellite to take a picture every time it passed over." During international conflicts this greater access could lessen the information advantage the United States has over other countries.

Some experts argue that expanded access could be beneficial. Neighboring countries might be less quick to threaten each other when troop movements were visible to all. When U.S. troops are involved in international conflicts, though, the U.S. government has a strong interest in controlling the flow of information. "One reason we were able to best the Iraqis," Williamson says, "was that we had very good information about them and they didn't know what we were doing."

To minimize security risks, the U.S. government is working to keep "shutter control"—broad latitude to turn off sensors when images might compromise "national security, international obligations and/or foreign policies." Representatives of television networks and other

news media argue that the government's authority to stop the use of satellite images should be no broader than its authority to stop the publication or airing of other sensitive information, and that exercising it should require the same judicial process.

Whatever the outcome of that debate, growing international competition means that customers who want high-resolution images will probably be able to buy them. The CIA has been cautious about declassifying spy-satellite pictures: so far only archives from 1960 to 1972 have been released to the public, and the results of a joint U.S.-Russian effort to study environmentally important sites around the world using spy satellites will be kept secret for the foreseeable future. But Russia is already selling some current two-meter images from military satellites, and France, Israel, and Japan plan to market high-resolution imagery.

WHERE to draw the line between personal privacy and the public and commercial need for information will become urgent when high-resolution surveillance is routine. For the first time, detailed pictures of every piece of private property in the United States will be routinely compiled and marketed. Commercial satellites cannot yet produce images of people, but they can show vehicles parked in driveways and structural changes to homes. They can provide images within a few hours and exact comparisons of the same property at precise intervals without giving clues about their presence—things that aerial photography cannot do.

For the police, precise images mean a new investigative tool, says James Frelk, the vice-president of EarthWatch, the company that plans the first new satellite launch. Officers monitoring a suspected crack house, for example, will be able to see the pattern of vehicles arriving and leaving. "They can see the difference between a van, a truck, and a car," Frelk says, "and make a good guess about whether the same car was there yesterday." He expects local governments to be regular customers for other uses, such as updating tax assessments and spotting additions to homes and outbuildings that are in violation of building codes.

The Fourth Amendment to the Consti-

tution has traditionally been understood to protect homes and the areas immediately surrounding them from unreasonable government intrusion; laws of trespass have protected against snooping by businesses or individuals. In the days before electronic wizardry, that meant freedom from physical entry. When wiretapping and hidden microphones made intrusion possible without breaking down doors or climbing fences, the idea of privacy became more subjective. The Constitution was then taken to mean that areas where individuals have "a reasonable expectation of privacy," including homes and yards, must remain free of government intrusion—physical or electronic.

But in the past ten years judicial support for the use of aerial photography to spot marijuana crops in the war against drugs has left doubt about whether any outdoor space can be considered private. The last time the Supreme Court ruled on the question, in 1986, it upheld the legality of an aerial backyard search that produced pictures of a stand of marijuana plants, hidden from view on the ground by a ten-foot-high fence. In the war against drugs "one of the casualties has been the Fourth Amendment," says Yale Kamisar, a professor of constitutional law at the University of Michigan and a leading authority on privacy issues. Most constitutional scholars agree that increasingly sophisticated technology is no justification for lessening the protection of privacy in one's home and yard. Yet courts continue to uphold warrantless searches of yards by means of aerial surveillance, even though the searches would be illegal if the police jumped a fence. "We have much less privacy than we think," Kamisar says. "If the Fourth Amendment doesn't adapt to new technology, it's going to wither and die."

Corporate privacy, too, is shrinking. On the same day that it upheld the aerial search for marijuana plants, the Supreme Court ruled on a case in which inspectors from the Environmental Protection Agency sought entry without a warrant to the 2,000-acre Dow Chemical plant in Midland, Michigan, in order to check emissions from power plants and take photographs, and were denied it. The inspectors then rented a plane and took seventy-five color photos using an aerial mapping camera; the Court found that



Experience a Great Adventure!

Join us on a 6 or 13 day Caribbean expedition from \$650.

Call your travel agent for more information or 1-800-327-2601.

Windjammer Barefoot Cruises
P.O. Box 190120, Dept. 204, Miami Beach, FL 33119

BOOKS #1 ON TAPE®

World's Largest Selection



- Best Sellers on Cassette
- Full-length Readings
- Call for Free Brochure

(800) 626-3333

Box 7900-AT, Newport Beach, CA 92558

PROVENCE BASQUE PYRENEES TUSCANY AND THE CINQUE TERRE

CLASSIC JOURNEYS

Easy going walking, cultural and natural history tours:

- expert local naturalist and historian guides
- historic and charming inns and lodges • small groups

For a free color catalog call toll-free: 1-800-200-3887

NEW ZEALAND SWISS ALPS SWISS AND ITALIAN LAKES COSTA RICA

ITALY'S ADRIATIC COAST



Half Moon

Golf, Tennis & Beach Club
Montego Bay, Jamaica

See your travel agent or call 800-626-0592 • 809-953-2211

Member ERI/Heinz E. W. Simonitsch, Dir.

To drive more
confidently into
a future nobody
can predict, call
1-800-582-SAAB,
Ext. 200.

Some are content to watch as events unfold before them. But if you'd rather control your destiny, we suggest the Saab 9000 CS. Its 2.3-liter turbocharged engine will give you power on demand, and its superb handling provides quick response to any twists and turns that lie ahead. It also has a cavernous cargo space (56.4 cu. ft.). Which should provide enough room for whatever else the future holds.

Call for a free Saab Excursion Kit giving complete information on all our models. And the perfect Saab to find your own road.



The Saab Excursion Kit.

© 1996 SAAB CARS USA, INC.
www.saabusa.com

inspection using aerial photography did not violate the Constitution.

Confusing matters further, the Court left clues that government satellite surveillance might be an invasion of privacy even when aerial photography is not. The majority said that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant." In each of the two cases four dissenting justices thought that there should be more protection of privacy than the Court provided.

Other threats to privacy arise when scattered public information is combined with precise images of homes or farms. A new wing on a house, a trip to the Caribbean, and a few major purchases could together signal a change in lifestyle of interest to tax collectors, business partners, or ex-spouses. Farmers competing for high yields could profit from a week-by-week record of a neighbor's success in using irrigation, fertilizers, and pesticides. New satellites will make information accessible on personal computers within hours.

Congress and state legislatures have in some instances restricted the free flow of information among companies and between government agencies and companies. Self-restraint by businesses and government agencies, too, can go a long way toward avoiding consumers' worst nightmares. But advances in technology are running far ahead of efforts to limit their use. Any further privacy protection will have to be legislated. "Whenever privacy questions occur in the context of new technology, it takes a long time for the courts to respond," says Gilbert S. Merritt, the chief judge of the U.S. Court of Appeals for the Sixth Circuit, who wrote the appellate opinion upholding the EPA's aerial surveillance of the Dow Chemical plant. "The last issues arose with wiretapping. It's taken forty years to reach some kind of stability in that law."

MOST new information, of course, will not raise privacy questions. But on what terms will it be shared? Until now geographic data have been treated as a national resource. Only a few governments have been capable of

launching earth-observing satellites. The last generation of U.S. civilian satellites, the Landsat series, was financed by taxpayers, and most of its images are available to the public for the cost of duplicating the information. (Landsat images have been distributed commercially since 1985.) But the next group of earth-observing satellites is being financed and launched by private companies. Their images will be produced under contract, customized for clients, and made available at market prices. EarthWatch will retain the ownership of all its images, licensing their use by individual customers and restricting their reproduction, just as computer companies now limit the copying of software. Foreign governments, large corporations, and other paying clients will get exclusive rights to information they pay for—a big change. "Up to now, when we have acquired mapping information by contract, it has been in the public domain," says Gale TeSelle, who coordinates geographic data at the Department of Agriculture. "We give it away or we sell it as inexpensively as possible." TeSelle believes that by using such information to encourage farmers to fight erosion, for example, or to use a minimum of chemicals against pests, the government can "increase the conservation ethic."

None of these concerns should slow the next steps in mapping the earth. It is cause for celebration that we are entering a time of competitive, unpredictable exploration just when description of the seven continents seemed virtually complete. Amid budget pressures and privatization efforts, however, there is real danger that simple and familiar protections will be compromised. Whatever the public and commercial value of creating precise maps linking physical characteristics of residences with other publicly available information, the making of those maps should be limited by the traditional notion that a person's home and surrounding areas are private. And commercial satellite ventures should be limited by the idea that geographic information remains a national resource, to be shared at minimal cost. Dangers lie not in what satellite sensors can record but in how the political system allows that information to be used. The clearer the protections now, the greater the likely benefits later. ☺

Membership of the Privacy Working Group
Information Policy Committee
Information Infrastructure Task Force
August, 1996

Shari Alpert, Office of Privacy Advocate, Internal Revenue Service
Charles Chamberlain, Information Technology, US Postal Service
Scott Charney, Computer Crime Unit, Department of Justice
John Fanning, Office of Assistant Secretary for Planning and
Evaluation, HHS
Gerald Gates (Chair) and Fred Shenk, Policy Office, Bureau of the Census
Linda Joachim, FOIA/PA Unit, Department of Justice
David Medine and Martha Landesberg, Division of Credit Practices,
Federal Trade Commission
Kirsten Moncada, Office of Information and Privacy, Department of Justice
William Murphy, Office of General Counsel, Department of Treasury
Michelle Muth, U.S. Office of Consumer Affairs
Matthew Powell, Office of General Counsel, National Science
Foundation
Mary Ronan, Access Staff, National Archives and Records
Administration
Joyce Schaul, Office of Disclosure Policy, Social Security
Administration
Barbara Wellbery and Joanna Lowry, Office of General Counsel,
National Telecommunications and Information Administration



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Tim

AUG 16 1996

ADMINISTRATOR
OFFICE OF
INFORMATION AND
REGULATORY AFFAIRS

MEMORANDUM FOR THE INFORMATION INFRASTRUCTURE TASK FORCE (IITF)

FROM:

Sally Katzen *Sally Katzen*

SUBJECT:

Privacy Working Group Draft Report -- "Options for Promoting Information Privacy on the National Information Infrastructure"

Enclosed for your review and comment is a draft report prepared by the Privacy Working Group of the IITF's Information Policy Committee. This draft is the result of extensive discussion and analysis by the working group, chaired by Gerald Gates of the Census Bureau. A list of the members of the working group is attached for reference. The report is an options paper. It contains no recommendations and conveys no decision regarding any of the options it presents. Indeed, it should be emphasized that the report has not been reviewed by Administration policy officials.

The working group will shortly seek public comment on its paper so that policy officials may have the benefit of that input before making decisions. Before the working group publishes the report in the Federal Register, however, I would like to have the benefit of any comments from the IITF. In the interests of time, I am soliciting the comments of the IITF's Information Policy Committee and the full IITF concurrently.

Please provide comments no later than September 6, 1996. To the extent practicable, please provide line-in line-out comments. The working group will resolve the comments with the assistance of the Information Policy Committee. The working group will then publish the resulting report in the Federal Register for comment. Your comments should be sent to: Mr. Gerald Gates, Policy Office, Room 2430, Building 3, Bureau of the Census, Washington DC 20233. Phone: (301)457-2515; FAX: (301)457-2654.

Attachment

cc: Information Policy Committee
Gerald Gates

Options for Promoting Privacy on the National Information Infrastructure

A DRAFT REPORT
OF THE
PRIVACY WORKING GROUP
INFORMATION POLICY COMMITTEE
INFORMATION INFRASTRUCTURE TASK FORCE

June 28, 1996

A hml day
Jan Leary

Market - large scale privacy
in such common
privacy protection?

P3 - What makes it different?
- RLS/Redundant - commercial

- What are the principles

- When ~~data~~ it can, make

person a or who he expects?

EXECUTIVE SUMMARY

In this White Paper, the Privacy Working Group of the Information Infrastructure Task Force responds to concerns about personal information privacy. As the National Information Infrastructure (NII) develops, more and more individuals will use it for a wide range of purposes. As the NII and other developing technologies increase the utility of personal information to public and private entities, it becomes increasingly important to secure a proper balance between individuals' personal privacy interests and society's information needs.

This paper addresses these concerns in three ways. First, it provides an overview of the impact of emerging technologies on informational privacy. Second, it discusses in more detail the laws and policies affecting informational privacy in four specific areas --

- o Government Records (traditionally a source of concern),
- o Communications (which is heavily regulated),
- o Medical Records (for the most unregulated), and
- o The Marketplace (which is regulated in part).

Third, it analyzes the various factors and options that could be considered in choosing to retain the status quo, enhancing the Federal Government role under the current approach to information privacy, and creating some type of entity designed to focus on informational privacy issues.

The sharing of personal information will only intensify with the evolving NII. Indeed, information is currently collected, shared, aggregated, and disseminated at a rate and to a degree unthinkable even twenty years ago. Additionally, governments are no longer the sole possessors of extensive amounts of personal information about U.S. citizens -- recent years have seen a tremendous increase in the acquisition of personal information by the private sector. Although there have been some efforts at self-regulation and some legislative responses, the vast majority of personal information is not protected under Federal law and can be sold, shared, exchanged and disseminated without notice to or input by the individual. This has raised many privacy concerns among the American public which have been reflected in recent polls.

The more detailed discussion of the four selected areas

noted above, reveals that information privacy in the United States is currently a patchwork quilt of varying levels of protection based on the existence and nature of relevant laws and policies. For example, the titles of the videos an individual rents is afforded greater protection than extremely sensitive medical information concerning that individual. Moreover, the degree of protection for video records depends upon whether the movie is rented from a store or a cable company. That store rentals are protected at all is only because of a celebrated case involving the disclosure of such records. In sum, this portion of the paper demonstrates that the history of information privacy protection in the United States is generally a reactive one, where legislation or policies are enacted or adopted in response to a specific identified harm and only after a particular privacy issue has become problematic.

As we have seen from the discussions throughout this paper, the United States has no legally defined comprehensive right to informational privacy that spans both the public and private sectors. The gaps between laws/policies and current practices establish the framework for our analysis of possible Administration options. In Section IV, we consider three such options in attempting to answer the core question: can we do better in balancing the needs of government, commerce, and individuals, keeping in mind both the interest in the free flow of information and the protection of informational privacy? The three options are: (1) maintain the status quo, with the current mix of policy and legislative initiatives; (2) enhance the current federal government role under the status quo; and (3) create a privacy entity that would serve as a centralized focal point for informational privacy issues. In discussing each option, consideration is given to the upsides and the downsides of that option.

In considering the first option -- maintaining the status quo -- we have looked at recent efforts by Government agencies and business organizations to apply fair information principles to current practices. We also considered, in very general terms, state efforts to protect informational privacy. We have found that certain agencies have been quite active in the privacy arena and are spearheading efforts to push privacy to the forefront of business policy making. Additionally, we have found affirmative efforts on the part of the business community to address privacy concerns.

At the same time, however, we have found that privacy is often dealt with in a piece-meal and/or reactive manner in both the public and private sectors. For example, some areas of privacy concerns are not within any particular agency's purview and other areas of privacy straddle one or more agencies. Furthermore, no agency currently involved with privacy issues has privacy as even its primary, much less its only mission. Likewise, in the private sector, changes in privacy practices often occur in response to some precipitating event and there is currently in place no one focal point to assist business in identifying and responding to the myriad privacy issues facing the private sector in an increasingly networked world.

Encryptions
In discussing the second option -- enhancing the current government role under the status quo -- we consider whether current privacy protection efforts could be supplemented or enhanced to afford a more cohesive and proactive response to informational privacy issues. In considering this option, we note that both government and private industry have recently become more active with respect to privacy. Although these recent efforts can arguably be viewed as falling within the status quo already addressed in option one, this option explores the possibility that such efforts could result in privacy becoming a market commodity in the Information Age. As government and consumers become more aware of the NII's data collection, analysis and distribution capabilities, demand for privacy protection could result in a robust, competitive market for privacy protection. This option also considers ways in which Government could facilitate the development of this privacy market (i.e., getting its own house in order, playing a larger role in consumer and business education, and enhancing self-regulation by exploring enforcement deficiencies with industry).

*MCH
DWH
0/12*
At the same time, however, we recognize that this option may well be viewed as little more than the status quo approach in a different package. Second, it would not change the current sectoral approach to privacy. As discussed throughout this White Paper, the current framework of piecemeal legislative efforts and sectoral approaches leads to inconsistent privacy protections and does not anticipate future developments in a comprehensive and proactive manner. Furthermore, the enhanced government efforts envisioned under this option would arguably be facilitated more by an overarching vision for how privacy can best be protected than by maintaining and "beefing up" the current sectoral

framework. A centralized focal point for addressing privacy concerns could permit agencies to maintain their current spheres of responsibility while facilitating these agencies' identification of and response to a myriad of privacy issues in a comprehensive and coordinated manner. Finally, while recognizing that market forces play a critical role in protecting privacy, we caution against relying too heavily on market forces as the exclusive cure for any and all privacy related problems that may arise in an increasingly complex and networked world.

In considering the third option -- creation of a privacy entity -- we discuss the many forms that this option could take and consider the upsides and downsides of the various choices. We begin with a consideration of the functions that such an entity could perform. These range from advisory to regulatory with a range of functions in between (i.e. educational, ombudsman, and representational). Functions are discussed at pages 60-65. We next discuss the potential placement of such an entity considering placement as an executive branch agency, a federal spokesperson, an independent regulatory commission, an advisory committee or within an already existing agency. Placement is discussed at pages 65-70. Finally, we consider whether the sphere of influence for the entity should include the Federal government, the private sector or both (pages 70-72) and we address its composition at page 72. Finally, Appendix A sets forth, in tabular form, the function and placement choices for a privacy entity and also sets forth some sample decisional trees for the creation of such an entity.

TABLE OF CONTENTS

I.	PRIVACY DEFINED	2
II.	EMERGING TECHNOLOGIES AND THEIR EFFECT ON INFORMATIONAL PRIVACY	3
III.	A SURVEY OF FOUR ZONES OF INFORMATIONAL PRIVACY	10
	A. INTRODUCTION	10
	B. PRIVACY OF FEDERAL GOVERNMENT RECORDS	13
	C. PRIVACY IN COMMUNICATIONS	17
	1. Real-time Communications	17
	2. Stored Communications	19
	3. Toll Records and Other Subscriber Information	21
	4. Laws Protecting the Privacy of Mail	24
	D. PRIVACY IN MEDICAL RECORDS	25
	E. PRIVACY IN THE MARKETPLACE	31
	1. Personal Financial Condition	31
	2. Video Rental Record Privacy	43
	3. Direct Marketing	45
IV.	OPTIONS FOR PROTECTING INFORMATIONAL PRIVACY ON THE NII	50
	A. MAINTAINING THE STATUS QUO	51
	B. ENHANCED GOVERNMENT ROLE UNDER THE STATUS QUO	56
	C. CREATION OF A PRIVACY ENTITY	59
	1. Functions	60
	a. The Regulatory Function	60
	b. The Advisory Function	61
	c. The Educational and Research Functions	62
	d. The Ombudsman Function	62
	e. The Coordination and Representational Functions	63
	2. Placement	64
	a. Placement of the Entity Within the Executive Branch - Executive Agency or Federal Spokesperson	64
	b. Placement of the Entity Outside the Executive Branch - Independent Regulatory Commission	66
	c. Placement of the Entity Within an Already Existing Agency	68
	d. Placement of the Entity as an Advisory Committee	68
	3. Sphere of Influence	69
	4. Composition	71
V.	CONCLUSION	71
	APPENDIX A	A-1

PREFACE

The Privacy Working Group (PWG) of the Information Infrastructure Task Force was convened to determine the likely effect of the implementation of the National Information Infrastructure (NII) on individual privacy and to recommend actions to ensure public trust in its use. The PWG's first project involved the development of new fair information principles, and resulted in the Information Infrastructure Task Forces's Principles for Providing and Using Personal Information. Now, we have begun to look at whether the country would benefit from the creation of a Privacy Entity, an entity focusing exclusively on privacy issues. This White Paper is divided into Five Sections:

- SECTION I: PRIVACY DEFINED, discusses the concept of Privacy in general.
- SECTION II: EMERGING TECHNOLOGIES AND THEIR EFFECT ON INFORMATIONAL PRIVACY, provides an overview of informational privacy in the modern networked world.
- SECTION III: A SURVEY OF FOUR ZONES OF INFORMATIONAL PRIVACY provides a more detailed discussion of laws and policies affecting informational privacy in four specific areas (Government Records, Communications, Medical Records and the Marketplace).
- SECTION IV: FUNDAMENTAL CONSIDERATIONS OPTIONS FOR PROTECTING INFORMATIONAL PRIVACY ON THE NII is the section of the Paper that addresses the various options for protecting privacy in the new networked environment. These include maintaining the status quo, implementing new privacy initiatives under the current privacy framework, and creating a privacy entity.
- SECTION V: Sets forth the Conclusion
- APPENDIX A: Sets forth in tabular form the various options available for function and placement and provides some sample decision trees based on the Privacy Entity option.

I. PRIVACY DEFINED

That we were tasked with determining the need for a Privacy Entity (hereinafter, "PE") suggests concern about "privacy" and, more particularly, that the NII might erode it. Whatever "privacy" is--and there are several common definitions--it is of considerable concern to Americans: public opinion polls conducted over the past several years have shown an increasing concern with privacy-related issues.¹

For legal purposes, there are at least four different definitions of privacy:

- o intrusion upon the individual's seclusion or solitude, or into his private affairs;
- o public disclosure of embarrassing private facts about the individual;
- o publicity that places the individual in a false light in the public eye; and
- o appropriation, for another person's advantage, of the individual's name or likeness.²

Although such legal definitions are necessary for enforcing legal rights, an individual's interest in privacy is not so narrowly restricted. For example, Communications Canada defines privacy to include not just the right to be left alone and to control information about oneself, but also the right to remain anonymous.³ This more expansive definition highlights the difficulty in applying existing privacy standards to an electronic environment such as the NII. For example, allowing anonymity in the context of telephone voice communications poses only a minimal risk to society because conversations generally involve only a small finite number of individuals. Therefore, the type of harm that can be caused in any one call, such as an obscene or threatening call, is similarly limited. By comparison, anonymity in a networked electronic environment raises far different societal concerns. For example, because of its reach, the NII permits libelous statements to reach a far

¹ See discussion of HARRIS-EQUIFAX CONSUMER PRIVACY SURVEY, *infra* n. 20.

² See William Prosser, "Privacy," 48 CALIFORNIA LAW REVIEW, 1960, at 383.

³ See Communications Canada, TELECOMMUNICATIONS PRIVACY PRINCIPLES, December 1992, at 5.

broader audience at less cost than ever before possible.⁴

Although each of the above definitions differs in scope, "virtually every definition of privacy expresses one central concept--that privacy is the claim of individuals to decide what information about themselves will be communicated to others."⁵ There are, however, inherent limitations in this right. For example, individuals cannot suppress public records, nor control information about themselves that, by law, is used for a permissible purpose (e.g., a criminal defendant cannot prevent a court from examining his/her prior criminal record before imposing sentence and a seller of realty cannot prevent a title search of his/her property). Likewise, although individuals can attempt to control the dissemination of information about themselves by refusing to disclose certain facts, such disclosure is often either required by law (e.g., tax information) or required if the data subject hopes to participate in society in a meaningful way (e.g., releasing financial information to obtain a mortgage or releasing medical information to obtain insurance coverage).

As a result, the amount of information that is needed, used, and available about each individual is virtually limitless, and individuals cannot participate fully in society without disclosing vast amounts of personal data. Thus, the critical question becomes: how do we balance the need to use information (by government, commerce, and individuals) with the right of individuals to decide what information about themselves will be exposed to others?

II. EMERGING TECHNOLOGIES AND THEIR EFFECT ON INFORMATIONAL PRIVACY

The sharing of personal information will only intensify with the evolving NII. As noted in the Privacy Principles, individuals will use the NII to communicate, order goods and services, and obtain information. But unlike paying cash in a store, using the NII for such purposes will generate data documenting the transaction that can be easily stored, retrieved,

⁴ Similarly, the Morris worm, which was designed by its programmer not to be traceable to its source, shut down approximately 6,000 computers in one day. It is difficult to think of a pre-network analogy with such profound consequences.

⁵ See Alan Westin, THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE, 1990, at p. XVIII.

analyzed and reused.⁶ Indeed, information is currently collected, shared, aggregated, and disseminated at a rate and to a degree unthinkable only twenty years ago and this trend will continue as the NII evolves.⁷ Furthermore, while privacy concerns in the United States have traditionally arisen in connection with data collection by the government, governments are no longer the sole possessors of extensive amounts of personal information about U.S. citizens.⁸ In past years, we

⁶ IITF Privacy Working Group, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION, June 6 1995 at 1.

⁷ For example, we are all familiar with situations in which we must currently divulge personal information in order to obtain goods and services (e.g., obtaining a drivers license, cashing a personal check, using an Automated Teller Machine, applying for a mortgage, etc.). However, what the NII and other future applications of information technologies will present us with may not fall neatly within our current experiences. For instance, new applications of technology on the nation's roadways potentially will allow extensive monitoring and tracking of identifiable vehicles being driven almost anywhere. Features on some Worldwide Web browser software can compile small electronic dossiers on the Internet browsing and buying habits of Web users, and are accessible by the various Web sites visited. Applications of biometric identification and the capture of dynamic digitized signatures are increasingly being used. All these examples illustrate the fact that new technologies, while having positive uses, may also threaten privacy interests, if these interests are not carefully considered before technology applications are designed and implemented.

⁸ For example, Acxiom Corporation, one of the nation's leading data management and marketing consultants, maintains approximately 350 terabytes of information about consumers (one terabyte being equivalent to 500 million pages of single-spaced text). See Elisa Williams, "Mining for Megadata// Mountains of Customer Information are Constantly Being Formed and Tapped," THE ORANGE COUNTY REGISTER, April 22, 1996, (1996 WL 7023685). Equifax, one of the credit reporting industry's big three, has announced plans to develop medical records databases and is already storing some health claims data. See John Riley, "Changes in Health Care are Eroding Medical Records Privacy Protection," NEWSDAY, April 23, 1996 (1996 WL 9903637); Jay Greene, Your Medical Records - Perhaps Your Most Personal Information - Also are the Most Vulnerable to Public Scrutiny," THE ORANGE COUNTY REGISTER, April 24, 1996 (1996 WL 7023964). The Medical Information Bureau maintains health and related records on 15 million Americans (Id.) and the credit reporting industry maintains records on approximately 190 million Americans. See Ann Merrill, "Credit

have witnessed a tremendous increase in the acquisition of personal information by the private sector, as consumers more frequently purchase goods with plastic (leaving a trail of charges), buy new services (such as pay-per-view movies), and engage in an ever greater number of miscellaneous electronic transactions (e.g., e-mail). All types of information about individuals are routinely gathered from numerous sources, aggregated, and shared. Furthermore, businesses often collect this information in ways that are not readily apparent to the individual.⁹

Bureaus Continue to be Leading Source of Complaints About Privacy," MINNEAPOLIS ST. PAUL STAR-TRIBUNE, February 1, 1996 (1996 WL 6900979).

⁹ Four examples illustrate the point:

- (1) Calling an "800" or "900" number permits the party receiving the call to identify the caller's number through Automatic Number Identification. Using a reverse directory in turn leads to identification of the caller's address. This information can then be compiled into a computerized list that can be sold to other marketers. Reported in Peter Sinton, "Perils Await the Unwary on the Cyber-Frontier," THE SAN FRANCISCO CHRONICLE, February 7, 1995 (1995 WL 5262597); Connie Koenenn, "How they Get Your Number - From You," THE CHICAGO SUN-TIMES, September 15, 1993 (1993 WL 6549139).
- (2) Likewise, attending a hospital sponsored seminar, health fair or health screening can result in an individual being placed on a list for marketing purposes. Hospitals subsequently use these lists of names for "mailings or telephone calls soliciting business for the hospital." Reported in "Using Medical Information for Marketing," PRIVACY JOURNAL, Vol XVI, No.4, February 1990, at 1.
- (3) Even shopping at the local supermarket can create a detailed computerized list that contains the exact nature and frequency of an individual's purchases. Connie Koenenn, "Junk Mail: Guess Who's Giving Out Your Address," LOS ANGELES TIMES, June 17, 1993 (1993 WL 2303036). See also, Carrie Teegardin, "Keeping Tabs on Shoppers A&P Membership Card Records Each Purchase in a Database," THE ATLANTA JOURNAL-CONSTITUTION, July 2, 1994 (1994 WL 4469745) (reporting on supermarket computerized membership cards and on the discontinuance of such a program, instituted in groceries in several cities, due to customer anger over the fact that detailed shopping data about the customers was being sold to anyone willing to pay for it).
- (4) A 1990 General Accounting Office report found that the private sector, as well as state and local agencies obtains

Modern technology is making it easier to integrate data from numerous sources to create a much more powerful information package about an individual than was previously possible. This increased capability, in turn, threatens privacy because control over personal data is lost and problems with data errors are greatly exacerbated.¹⁰ Indeed, the continual acquisition and compilation of personal information results in the creation of what can be viewed as an individual's "ELECTRONIC CLONE."¹¹ This clone, which exists in digital form, provides an intimate and detailed insight into an individual's medical condition, buying habits, personal tastes, economic bracket, vacation choices, ethnic background, political and religious affiliations, and even into how that person thinks (e.g., the causes and programs which he/she supports through contributions).¹² According to the publisher of the Standard Rate and Data Service, a catalog of mailing lists, there are at least 17,000 mailing lists and, although estimates vary, privacy experts believe those lists track more than 2 billion names. The average American is on at least 25, and as many as 100 of these lists at any one time.¹³

information contained in federal government databanks. See nn. 39-40 *infra*.

¹⁰ H. Jeff Smith, *MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA*, The University of North Carolina Press, 1994, at 7-8 and at 124-25 (discussing the distinction between information existing in separate, distinct pieces and the same information combined and available in one place).

¹¹ "As we see a convergence between telecommunications, computers and information processing, almost any transaction you enter into is leaving some kind of trace." Comments of Fordham University School of Law professor Joel Reidenberg, reported in Kinsey Wilson, "Your Life as an Open Book - Digital Wizardry that Promises to Make Life More Convenient Could Threaten your Privacy," *NEWSDAY*, July 21, 1993 (1993 WL 11382702).

¹² For a representative sampling of the types of databases that are being compiled and the kinds of information they contain, see Thomas B. Rosenstiel, "Someone May Be Watching - Everywhere We Go, We're Increasingly Under Surveillance. Employers, Marketers, even Private Detectives Use High-Tech Tools and Scan Mostly Unregulated Databases to Pry into our Daily Lives," *LOS ANGELES TIMES*, May 18, 1994 (1994 WL 2166435); Larry Tye, "List-Makers Draw a Bead on Many," *THE BOSTON GLOBE*, September 6, 1993 (1993 WL 6607597).

¹³ Reported in Jay Greene, "They're Selling Your Secrets," *THE ORANGE COUNTY REGISTER*, April 21, 1996 (1996 WL 7023494). See also, Jim Donaldson, "You Can Keep Your Privacy But it Will Take Some Doing," *GANNETT NEWS SERVICE*, March 6, 1996 (1996 WL 4375432)

Not surprisingly, this situation has concerned some commentators. For example, David F. Linowes, former chairman of the Privacy Protection Study Commission, has stated that:

Without our knowledge we are profiled and placed on many specialized lists, whether we like it or not. You could be classified as a foreign policy hawk, affluent ethnic professional, black activist, person who frequents the dice table. You don't know what lists you are on.¹⁴

Although some industries have pursued self-regulation through codes and principles and there have been some legislative responses to protect personal information, the vast majority of personal information currently can be sold, shared, exchanged and disseminated without notice to or input by the individual.¹⁵ A recent study of seven organizations found that corporate privacy policies are often inadequate and that even where such policies exist, a significant policy/practice gap exists (i.e. the actual practices are not consistent with announced policies).¹⁶ The ever increasing demand for personal information coupled with the almost limitless ability to acquire, aggregate, share, and disseminate this information facilitates its misuse and abuse, notwithstanding the good intentions of legitimate data collectors. This has raised privacy concerns among the American public; recent polls reflect a growing public concern with information privacy issues.¹⁷

(reporting that the typical shopper is in at least 25 corporate databases).

¹⁴ Reported in Mary Zahn and Eldon Knoche, Electronic Footprints Yours are a Lot Easier to Track than you may Think MILWAUKEE SENTINEL, January 16, 1995 (1995 WL 2967415).

¹⁵ See generally, G. Bruce Knecht, "Privacy: A New Casualty in Legal Battles," THE WALL STREET JOURNAL, April 11, 1995 (reporting on the "data that is held -- in staggering amounts -- by private-sector companies" and on the fact that "[v]ast amounts of consumer information are entirely unprotected").

¹⁶ See MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA, supra n.10, chapters 3 & 4.

¹⁷ Although in a 1995 Equifax-Harris poll, the percentage of respondents concerned with protecting the privacy of consumer information (61%) ranked behind such things as reducing insurance fraud (74%) and controlling the cost of false advertising (71%), it still placed fifth among nine different consumer issues covered in the poll. Additionally, the 1994 and 1995 Equifax-

Although individuals disagree on the extent to which the collection and use of information should be limited to protect privacy, most agree it is appropriate to engage in a careful weighing of benefits and harms. The Privacy Principles acknowledged this balancing process in stating "that privacy interests are not absolute and must be balanced by the need for legal accountability, adherence to the First Amendment, law enforcement needs, and other societal benefits recognized in law."¹⁸

Appropriate uses of information can create significant opportunities for both the data subject and society as a whole. For example, the use of databases containing personal information about consumers may allow a company to enter the marketplace by identifying individuals likely to want a particular product. This may not only provide the data subject with desired goods and services, but may also increase competition and lower consumer costs generally. Government use of such lists may serve to ensure that citizens receive benefits that they need while minimizing payment of fraudulent claims. Using medical information for research purposes may help cure diseases.

Inappropriate uses of information creates an equally lengthy list of harms. Misuse of medical information may decrease employment opportunities (e.g., denying an individual a job because of an old but stigmatizing medical condition, such as depression), improper use of demographic information may result

Harris surveys revealed that 84% and 82% respectively of the individuals polled expressed concern about threats to personal privacy. This is an increase from the 79% in 1990 and 1993 and the 64% in 1978. Furthermore, of those surveyed in the 1990 poll, 71% said they believed consumers had lost all control over how personal information about them is circulated and used by companies. In 1995 that number had risen to 80%. Likewise, in 1990 42% of the people polled indicated that they have at some point refused to give information to a business or company because they thought it was either not really needed or was too personal. By 1995, that number had risen to 59%. However, of those surveyed in the 1995 poll, 17% agreed strongly and 40% agreed somewhat that businesses handling personal information were paying more attention to privacy issues. Additionally, both the 1995 and 1994 polls indicated that more people are worried about privacy invasions by government agencies than by businesses (in 1995 the ratio was 51% to 43% and in 1994 it was 52% to 40%). Finally the proportion of people agreeing that technology has almost gotten out of control is higher than it has ever been (63% in the 1995 poll versus 53% in 1994, 50% in 1993, 45% in 1990 and 43% in 1978).

¹⁸ Privacy Principles, supra n.6, at 2.

90
Bund

in redlining, and the inappropriate disclosure of personal information may cause embarrassment or even harassment. Additionally, the magnitude of information collection, storage, and dissemination increases the probability that information will be used in a manner and for a purpose not reasonably contemplated by the information provider. The Privacy Principles have recognized the need to give consideration to "the individual's expectations regarding the use of the information."¹⁹

Ultimately, the appropriateness of any given use of information must be considered on a case-by-case basis. In extreme cases at either end of the continuum, separating acceptable uses (those that maximize opportunity with minimal impact upon privacy) from unacceptable uses (those that severely reduce privacy with little or no benefit) may not be difficult. Most cases, however, fall in the middle of the spectrum, and weighing the information use benefit against the privacy harm is by no means clear or easy. In the absence of laws or regulations to resolve this conflict (such as the Privacy Act's restrictions on cross-matching or the Video Privacy Protection Act's prohibition on disclosing video sale or rental records), the decision to use information remains in the hands of information possessors. Their decisions about its use, however, will be influenced by, among other things, market forces, operating efficiencies, law enforcement efforts, and civil liability.

Finally, the vast accumulation and dissemination of personal information in the United States without notice to or input by the information provider today may eventually impact more than the individual consumer. Many European countries currently have data protection laws and the European Union recently has formulated a directive regarding informational privacy (the EU Directive).²⁰ Commentators have noted both the difference between the U.S. and European approach to information privacy protection and the difficulties this difference may pose for American businesses if the disparity continues to exist.²¹

¹⁹ Id.

²⁰ See European Union, DIRECTIVE 95//EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, July 20, 1995.

²¹ See, the SIXTH CONFERENCE ON COMPUTERS, FREEDOM AND PRIVACY recently held in Cambridge, Massachusetts, where it was announced during conference sessions that 17 of the 24 OECD countries had enacted a "comprehensive data protection statute, overseen by an independent oversight agency," that Hong Kong had adopted a law closely modeled after the European Union's Data Protection Directive, and that of the 7 OECD countries that had still not

Of course, it is important not to lose sight of the core dichotomy: while information's value lies in its use, the use of information may diminish privacy. As developing technology makes us an increasingly information dependent society, it becomes increasingly important to strike a proper balance between the individual's personal privacy interests and society's information needs.²²

Thus, we turn to a consideration of current efforts to protect privacy. It would be beyond the scope of this work to attempt to catalog and discuss every privacy law, or every substantive privacy issue. Instead, we focused on four critical areas or zones that serve to provide a broad view of privacy issues and societal responses:

- (1) Privacy of Federal Government records (a traditional source of concern),
- (2) Privacy in Communications (heavily regulated),
- (3) Privacy of Medical Records (for the most part, unregulated), and
- (4) Privacy in the Marketplace (which is regulated in part and subject, in some cases, to extensive industry imposed codes of fair information practices).

III. A SURVEY OF FOUR ZONES OF INFORMATIONAL PRIVACY

A. INTRODUCTION

Before addressing the four zones of information privacy listed above, it is important to offer some preliminary comments about the protection of privacy generally. Because privacy is

adopted a comprehensive data protection statute, such a law was "firmly on the agendas" of all of these countries with the exception of the United States. Reported in NEWSBYTES - Computers & Privacy - World Governments Tackle Web, April 1, 1996 (1996 WL 8906565). See also, comments of Professor Joel Reidenberg that the European Community is developing a protocol for how business and government can use personal information and that U.S. trade could suffer if European nations are barred from dealing with companies that do not abide by the protocol. Reported in Kinsey Wilson, Your Life as an Open Book - Digital Wizardry the Promises to Make Life More Convenient Could Threaten Your Privacy, NEWSDAY, July 21, 1993 (1993 WL 11382702).

²² See Privacy Protection Study Commission, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, June 1977, at 3.

such a broad concept and the use of information is such a complex issue, it is generally not feasible to attempt to protect privacy by implementing one overarching all-inclusive privacy law. Indeed, many privacy experts agree that, to the extent regulation or legislation is warranted, a sector by sector approach is the only viable method of protecting privacy. Protecting privacy in an increasingly networked environment, however, requires far more than regulation--it requires reliance on a variety of tools designed to ensure that information is used properly. Social customs, education, market forces, courts, enforceable industry codes of conduct, and the use of computer security techniques may all play a significant role in ensuring that information is used only for acceptable purposes.

Each of these techniques may offer a different level of protection, and may provide a different remedy when a privacy infraction occurs. If a social custom--normally articulated as "fair information principles"--is violated, the penalty may be embarrassment or ostracism. Market forces may cause a company that inappropriately sells personal customer information to lose business to a competitor with different information practices. Failure to follow accepted computer security standards might result in civil liability. Failure to follow legal requirements may result in civil or even criminal penalties. Although this framework seems clear and workable in the abstract, it is difficult to apply in practice because, as noted previously, most uses of information fall within a grey area between clearly acceptable and clearly unacceptable. Fair information principles provide guidance, but what constitutes "fairness," especially under the NII umbrella, may be neither clear nor intuitive. For example, a doctor who uses the dates of birth in his patients' records to send birthday cards to his patients and tell those over a certain age that they now qualify for senior citizen discounts may offend some individuals but be applauded by others, thus suggesting that whether a particular information use is fair may sometimes be a matter of opinion.

Traditionally, fair information practices that are enforced by legal sanctions (i.e. laws which impose some limitations on the use of information) are fairly specific, since it would be unfair to apply such sanctions if the actor's conduct was not clearly prohibited. As a result, most privacy laws deal only with a particular type of information, and then only when that information is held by a particular sector (e.g., financial records held by financial institutions, video purchase/rental records maintained by those who sell or rent videos, credit reporting records maintained by credit bureaus).²³ Furthermore,

²³ Two notable exceptions are the Electronic Communications Privacy Act, which broadly protects communicative privacy, and the Privacy Act of 1974, which applies to records held by Federal

in privacy matters, legislators generally have been more reactive than proactive, passing laws in piecemeal fashion in response to a specific event or concern and without careful consideration of preexisting privacy laws.²⁴ This results in inconsistent protection for similar types of records. For example, a law enforcement agency can obtain records from a video rental provider with a grand jury subpoena, but this same information cannot be obtained from a cable company unless a court order is obtained. And there is often no logical relationship between the protection afforded and the sensitivity of the information protected. For example, under current Federal law, the names of the videos an individual rents is afforded greater privacy protection than sensitive and highly personal medical information about that individual.

In the absence of comprehensive privacy legislation, voluntarily enacted privacy policies also have helped to strike a balance between the individual's personal privacy, including maintaining the accuracy, confidentiality, and integrity of electronically stored personal data, and the many benefits of electronic exchange of personal information. However, the same piecemeal and reactive approach that limits the effectiveness of legislation also reduces the effectiveness of private sector policies. As with the legislative response, these policies also tend to arise in response to a specific situation or event. For example, one recent study described the policy making process as "a wandering and reactive one" with policies that "were poorly formed and improperly implemented" and where leadership on information privacy issues occurred only in response to some external threat, such as negative publicity or legislative scrutiny. This same study, however, observed that "today's economic and legal environment offers companies little incentive to lead in these matters."²⁵ Thus, even when laws and policies are juxtaposed, privacy is often not protected.

In sum, we need to consider whether the broad range of existing mechanisms, which currently balance the need to use information with the need to maintain informational privacy, strike the appropriate balance. In the sector discussions that follow, we start with legal restrictions that bind information

agencies in a system of records.

²⁴ This has led one commentator to note that no cohesive legislative framework has ever been created for privacy and that neither the business community nor privacy advocates can rely upon present U.S. law to resolve the majority of privacy disputes. See MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA, supra n.10, at 10.

²⁵ Id. at 55-56 and 92.

users and next discuss those internal sector policies and principles that supplement existing laws. Finally, we consider how successful this combination of law and policy has been in protecting informational privacy in an increasingly networked world.

B. PRIVACY OF FEDERAL GOVERNMENT RECORDS

Broadly speaking, the role of the Federal Government is to "establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity."²⁶ In support of this undertaking, the Federal Government coins money, collect taxes, regulates commerce, runs post offices, oversees immigration, funds social welfare programs, punishes crimes, and engages in a host of other activities designed to sustain the democracy itself (e.g., collecting the census to insure adequate representation in Congress based upon population figures) and protect the welfare of its citizens. Absent Federal preemption, state and local governments may address issues undertaken by the Federal Government (e.g., taxes, crime) and may handle those areas in which the Federal Government has no authority at all.

As a result of their broad and diverse responsibilities, governments maintain volumes of records on their own activities and on the activities of their citizens (e.g. census records, tax records, voting records, motor vehicle records, real property records, commercial records, criminal records, and even library records). Increased computerization of these records permits them to be used and analyzed in new ways which could pose a threat to privacy if no restrictions were in place.

Some legal protections, however, are already in place. For example, the confidentiality of Federal income tax returns and return information is currently protected by Federal law (see page 32 *infra*). Likewise, the confidentiality of decennial census records is protected by Federal law. Title 13 of the U.S. Code provides that information collected by the Census Bureau can be used only for statistical purposes, no information that could reveal the identity of a person or business can be released, and no one who is a Census Bureau employee, sworn to uphold the confidentiality of Title 13, can examine information that identifies individuals.

Records held by the public sector generally differ in two respects from those held by the private sector. First, since records collected and maintained by governments should be directly relevant to some particular governmental function, the amount and type of information collected is inherently limited by

²⁶ See U.S. CONST. Preamble.

factors other than the cost of collection and storage. For example, governments may by necessity collect and maintain tax records, but generally should have no need to collect the highly detailed financial records maintained by banks or credit card companies.

Second, unlike the private sector where records are scattered among numerous sectors and companies, in the case of government records one entity (i.e. the local, state or Federal Government) is ultimately responsible for the records, although they may be maintained by many different agencies or divisions. The result is a potential for consolidation. Considering the inherent power of government to affect the lives of its citizens, this clearly raises privacy concerns.

The Privacy Act

Against the backdrop of Watergate and increasing public concerns with government accumulation of information about individuals in large mainframe computers, Congress passed the Privacy Act of 1974.²⁷ The Act attempted to respond to public concerns about the Federal Government amassing centralized files on all its citizens by restricting the collection, use, and dissemination of personal information by Government agencies.²⁸

The Privacy Act applies to a wide variety of records maintained by Federal agencies, and is intended to protect privacy interests by regulating the Federal Government's collection, use, and dissemination of personal information. With one exception,²⁹ it applies only to Federal Government agencies, and does not cover state and local agencies, Congress, or the private sector. Moreover, it does not apply to all records maintained by a Federal agency, but only to those records retrieved by name or other personal identifier. An "individual" afforded protection under the Act is limited to U.S. citizens and aliens lawfully admitted for permanent residence. Foreigners, collective representatives such as unions, and corporations are not "individuals" for purposes of the Act.

Despite these limitations, the Act does provide some measure

²⁷ 5 U.S.C. § 552a. See generally James T. O'Reilly, FEDERAL INFORMATION DISCLOSURE, § 20.01 (2d ed. 1995).

²⁸ FEDERAL INFORMATION DISCLOSURE supra n.27 at § 20.01 at 20-5 (2d ed. 1995)--"Computerization had an essential role in passage of the Privacy Act because record retention systems were less threatening to the public and Congress when hand-held index cards required hours of search and retrieval."

²⁹ The exception is the social security number usage restrictions, contained in Section 7 of the Act, which apply to Federal, state, and local government agencies.

of privacy protection. For example, it establishes certain recordkeeping requirements that agencies must comply with, such as maintaining in its records only information that is "relevant and necessary" to accomplish a purpose of the agency, and maintaining all records used by the agency in making any determination about an individual in such a way as to assure fairness to the individual in that determination.³⁰ The Act further requires agencies to establish safeguards to ensure the security and confidentiality of records.³¹ The Act also regulates agency use and dissemination of information. For example, it prohibits disclosure without prior written consent of the individual unless the disclosure falls within certain enumerated exceptions although, admittedly, the list of allowable exceptions is extensive.³²

Individuals have rights and remedies under the Act. For example, individuals have the right to access agency records containing information about themselves, and the right to request amendment of information that is inaccurate, irrelevant, untimely, or incomplete.³³ Likewise, the Act provides for civil remedies including injunctive relief, and for criminal penalties for knowing and willful violations of the Act.³⁴

Notwithstanding its value, the Privacy Act has been widely criticized for falling far short of its drafters' expectations. One commentator has noted that "[t]he Act has produced mechanisms for coping with paperwork, instead of the altered behaviors of bureaucrats and individuals that were anticipated" and that "it became clear from several years of experience, the compromises and exceptions of the 1974 Act left the facade of a major bill of rights for individuals, but the working of a 'paper tiger' privacy statute."³⁵ Additionally, commentators have expressed concern about the Federal Government's relatively weak oversight of the Act.³⁶

³⁰ 5 U.S.C. § 552a(e)(1) and a(e)(5).

³¹ 5 U.S.C. § 552a(e)(10).

³² 5 U.S.C. § 552a(b)(1)-(11).

³³ 5 U.S.C. § 552a(d)(1) and § 552a(d)(2).

³⁴ 5 U.S.C. § 552a(g) and § 552a(i) respectively.

³⁵ FEDERAL INFORMATION DISCLOSURE, supra n.27 at 20-1 and 20-5.

³⁶ See, e.g. U.S. Congress, Office of Technology Assessment, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY, OTA-CIT-296 (1986) discussing deficiencies in

The Computer Matching and Privacy Protection Act

Technology has hardly been stagnant, and the Federal Government's move from mainframe computers to a network environment during the years following passage of the Privacy Act increased concerns about the government's ability to share and disseminate information about individuals once collected. Congress responded to these growing concerns by passing the Computer Matching and Privacy Protection Act of 1988.³⁷ This Act, which amends the Privacy Act, regulates Federal agency use and exchange of information contained in agency databases. The provisions add procedural requirements for agencies to follow when engaging in computer-matching activities, provide matching subjects the opportunity to receive notice and to refute adverse information before having a benefit denied or terminated, and require that agencies engaged in matching activities establish Data Protection Boards to oversee these activities. Finally, in 1990 Congress passed amendments to the Computer Matching and Privacy Protection Act which further clarified the due process provisions of the Act.

Commentators have continued to express concern about the Federal Government's accumulation and use of data. In 1990, the General Accounting Office reported on the significant aggregation and sharing of personal information by the private and public sectors.³⁸ The report found that computers and advanced technologies, such as computer networking, are widespread throughout the Federal Government and that Federal agencies both obtain information from and share information with third parties, including state and local agencies and the private sector.³⁹

OMB's oversight of Privacy Act implementation.

³⁷ Pub. L. No. 100-503.

³⁸ See General Accounting Office, COMPUTERS AND PRIVACY: HOW THE GOVERNMENT OBTAINS, VERIFIES, USES, AND PROTECTS PERSONAL DATA, (GAO/IMTEC-90-70BR) August 1990. The GAO prepared its report by sending detailed questionnaires to 189 Federal agencies, of which 178 agencies responded (i.e. a 94 percent response rate).

³⁹ The report found that some 78 percent of the 910 large computerized systems are networked through telecommunications facilities and that many of these systems can be accessed by a variety of Federal, state, and local agencies, as well as by private organizations. Report at 2, 10. The report also noted that 20 percent of the agencies responded that they collected personal information electronically from such sources as state divisions of motor vehicles, credit bureaus, and insurance companies and that 56 percent of the information in the agencies' 910 largest systems can be accessed by a variety of third parties such as other Federal agencies; state and local agencies; and

As noted previously, legal restrictions, which set minimum standards, are often supplemented by sector specific policies, and the Federal Government is no exception. In 1974 the Federal Government adopted Privacy Principles [i.e. Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, (Washington, D.C., Department of Health, Education and Welfare, 1973)]. Rapid advancements in computer technology in recent years, coupled with the integration of telecommunications and data processing, have dramatically altered the way information about individuals is obtained and used. New privacy principles issued by the Privacy Working Group in October 1995 have been published, but their impact is not yet clear.

C. PRIVACY IN COMMUNICATIONS

Few rights are more sacred than the right to communicate privately with other individuals, whether telephonically or by mail. In recognition of this fact, a sweeping law known as the Electronic Communications Privacy Act (ECPA) protects all real-time communications and stored transmissions (e.g., electronic mail and voice mail),⁴⁰ and separate laws protect the privacy of paper mail.⁴¹

1. REAL-TIME COMMUNICATIONS

ECPA prohibits eavesdropping on oral, wire, and electronic communications. Oral communications are protected when the speaker exhibits a reasonable expectation of privacy, such as a face-to-face conversation held in a private place such as a hotel room. Wire communications, which are phone calls, include conversations that travel in whole or in part by wire, and are understandable to the human ear. Finally, an electronic communication is any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate or foreign commerce, but does not include any wire or oral communication. Thus, the protection for electronic communications covers faxes and other types of data transfers.

Generally speaking, it is illegal to intercept the contents of any wire, oral, or electronic communication or to disclose the contents of a communication which one knows to have been

private organizations such as health care providers, marketing companies, and insurance companies. Report at 17-18.

⁴⁰ 18 U.S.C. § 2510, et.seq.

⁴¹ 39 U.S.C. § 3623(d).

illegally intercepted.⁴² There are, however, some significant exceptions to this rule. The most frequently used exceptions allow communications to be intercepted by: (1) a law enforcement officer if acting pursuant to a court order;⁴³ (2) any person, if a party to the communication gives consent;⁴⁴ (3) an employer, when acting in the ordinary course of its business;⁴⁵ and (4) a service provider when the provider is monitoring wire or electronic communications in the normal course of business as a necessary incident to the rendition of service or to protect the rights or property of the provider.⁴⁶

Although, from a privacy perspective, the distinction between wire and electronic communications has diminished in importance--individuals now use e-mail as frequently as the telephone--it is still significant in the law in two respects. First, voice communications can only be intercepted pursuant to a court order when certain designated offenses are committed.⁴⁷ By contrast, electronic communications can be intercepted when any Federal felony is being committed.⁴⁸ Second, the statutory exclusionary rule which broadly prohibits the use of communications unlawfully intercepted "in any trial, hearing, or other proceedings in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof" applies only to oral and wire communications; electronic communications are not covered by the

⁴² 18 U.S.C. § 2511.

⁴³ See 18 U.S.C. § 2516. To obtain such a court order, the government must show that both probable cause and necessity exist. To prove necessity, the government must show that "other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(c). Even after these requirements are satisfied and the interceptions begin, the government must actively "minimize" interceptions; that is, agents must stop listening (and stop recording) any conversation where criminal activity is not being discussed.

⁴⁴ 18 U.S.C. § 2511(c) and (d). Some states require two-party consent; that is, both parties to the communication must consent to the interception.

⁴⁵ 18 U.S.C. § 2510(5)(a).

⁴⁶ 18 U.S.C. § 2511(2)(a)(i).

⁴⁷ 18 U.S.C. § 2516(1)(providing list of offenses).

⁴⁸ 18 U.S.C. § 2516(3).

rule.⁴⁹

2. STORED COMMUNICATIONS

Voice mail and electronic mail (e-mail) services are protected under a separate section of ECPA.⁵⁰ First and foremost, it must be understood that the privacy protections provided by the statute to voice and e-mail apply only to messages "in electronic storage." This is a term of art, defined in the statute as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."⁵¹ Webster's New International Dictionary, Second Edition, defines "incidental" as "1. Happening as a chance or undesigned feature of something else; casual; hence, not of prime concern; subordinate." Thus, to be in electronic storage within the meaning of the statute, an electronic communication must be in storage as a by-product, or incidental feature, of the transmission of the message. Once the communication has been transmitted it may, of course, still be stored electronically, but it is stored subsequent to the transmission, for the purpose of maintaining a record. Accordingly, the definition of "electronic storage" is not satisfied. See United States Department of Justice, Federal Guidelines for Searching and Seizing Computers at 86-87 (1994).

To the extent the message is in electronic storage, the statutory scheme distinguishes between (1) voice mail and electronic mail; (2) public and non-public service providers; and (3) government and non-government requests for disclosure of the contents of electronic communications.

Under 18 U.S.C. § 2701, it is unlawful for anyone to intentionally access without authorization a facility through which an electronic communication service is provided, or intentionally exceed authorization to access that facility, and thereby obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage. Thus, the privacy of both voice mail and electronic mail are essentially protected against those who would access the contents of the communication without or in excess of authority.

If the service being utilized is a "public" provider, the provider itself is, with certain exceptions, prohibited by law

⁴⁹ 18 U.S.C. § 2515.

⁵⁰ 18 U.S.C. § 2701 et. seq.

⁵¹ 18 U.S.C. § 2510(17).

from disclosing the contents of communications in storage on its service. Anyone who provides an electronic communication service or remote computing services to the public, is prohibited by 18 U.S.C. § 2702 from voluntarily disclosing the contents of the electronic communications it stores or maintains on the service. A "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.⁵²

ECPA's Non-Disclosure Rule Has Exceptions

There are several important exceptions to § 2702's non-disclosure rule, including a provision under 18 U.S.C. § 2702(b)(3) allowing a person or entity to disclose the contents of a communication with the lawful consent of the originator, an addressee, or the intended recipient of such communication; a provision under § 2702(b)(5) allowing the service provider to disclose the contents necessary incident to its rendition of service or to protect the rights of the provider; and a provision under 18 U.S.C. § 2702(b)(6) allowing disclosure to a law enforcement agency if the contents were inadvertently obtained and appear to pertain to the commission of a crime.

It is not entirely clear what sorts of electronic communications services will be found to provide "public" service. Generally speaking, "public" means available to all who seek the service, even if there is some requirement, such as a fee. It is probably safe to assume that any service permitting "guest" or "visitor" access is "public." On the other hand, the term should not be read to cover business networks open only to employees for company business. If that business network is connected to the Internet (an extensive world-wide network), it may be part of a "public" system, but this does not necessarily mean that the corporate LAN (local-area network) becomes a "public" service.

For the government to obtain access to a "stored electronic communication," it must follow the dictates of 18 U.S.C. § 2703, which sets out different rules depending upon how long the particular communication has been in electronic storage. That section provides that "a governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage . . . for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant." 18 U.S.C. § 2703(a) (emphasis added). If the information has been stored for more than 180 days, prosecutors may use either a Rule 41 search warrant (without notice to the customer or subscriber) or an administrative subpoena, grand jury subpoena, trial subpoena,

⁵² 18 U.S.C. § 2711(2).

or a court order pursuant to 18 U.S.C. § 2703(d) (with notice to the customer or subscriber).

3. TOLL RECORDS AND OTHER SUBSCRIBER INFORMATION

The prohibitions on real-time interceptions and access to voice and electronic mail protect the contents of communications. But communications systems not only carry messages, they create records that reveal information about system users. Telephone toll billing records, for example, indicate what phone line was used to call what numbers, when, and for how long.

Prior to 1986, telephone toll billing records were not protected from disclosure under Federal law and the Federal Government routinely gained access to telephone toll records without any judicial process. Indeed, in Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court held that toll records could be obtained without use of a search warrant because a caller had no "legitimate expectation of privacy" protected under the Fourth Amendment in telephone numbers dialed.

The law was amended in 1986, and ECPA now protects such toll records.⁵³ As then passed, the law provided that a government entity could obtain "a record or other information pertaining to a subscriber to or customer of such service" only when the governmental entity used an administrative subpoena, grand jury subpoena, trial subpoena, search warrant, or a court order. Disclosure also could be made to the government with the consent of the subscriber or customer of such disclosure.

② On October 25, 1994, however, this standard was amended in part by the "Communications Assistance for Law Enforcement Act (CALEA),"⁵⁴ also known popularly as the "Digital Telephony Bill." The main purpose of the Digital Telephony Bill, which was heavily debated, is to require telecommunications carriers to design switches that will permit law enforcement personnel (1) to conduct court-authorized interceptions of wire and electronic communications handled by those carriers and, (2) to obtain call set-up information (transactional data about the call). The bill was needed because new digital switches, if not properly designed, would not be wiretappable.

Why change level of protection?

CALEA also strengthened the privacy rights of electronic communication service customers. Basic subscriber information--defined as the name, address, telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service

⁵³ 18 U.S.C. § 2703(c) (1) (C).

⁵⁴ P.L. 103-414.

and the types of services the subscriber or customer utilized-- can be obtained with a subpoena. To obtain other information (e.g., records of the addresses to which the subscriber has sent e-mail messages), the government must now use a search warrant or obtain a court order.⁵⁵ In either event, no notice to the subscriber or customer is required. Such information also can be obtained with the consent of the subscriber or customer.⁵⁶

2

Additionally, CALEA modified the ECPA standard for obtaining such a court order by raising the level of proof required. Under the pre-CALEA version, the Government could obtain such an order upon a showing that there was "reason to believe" that the information sought was "relevant to a legitimate law enforcement inquiry." Now, the government must present "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

ECPA Does Not Prohibit Sale of Data to Non-Governmental Entities

Exp 1
person
6/6/92
JMD

Although the ECPA specifically precludes electronic communications service providers from giving information to the government unless certain conditions are met, it does not preclude them from selling that data to non-governmental entities. The primary privacy concern in the telecommunications industry is the ease with which telecommunications-related personal information (or TRPI)⁵⁷ can be compiled. Communication providers in the course of transmitting communications among transacting parties have access to a wide variety of TRPI. These may be routing data, which may tell who communicated with whom at what time, day, and month, and length of transaction, and also billing records with all associated data. This electronic information can be easily monitored and copied, in a completely automated fashion, raising serious privacy concerns.

Available personal information may also include records of electronic purchases made over interactive networks, point-of-sale payments transacted electronically over networks, and even cable movies ordered and billed separately. The collection of TRPI, coupled with the increasing ease with which

⁵⁵ 18 U.S.C. § 2703(c)(1)(B)(i) and 18 U.S.C. § 2703(c)(1)(B)(ii).

⁵⁶ 18 U.S.C. § 2703(c)(1)(B)(iii).

⁵⁷ TRPI is not message content. See White Paper, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATION-RELATED PERSONAL INFORMATION, Office of Policy Analysis and Development, National Telecommunications and Information Administration, October 1995, at 5.

telecommunications service providers can sell such information when they perceive a market for doing so, raises additional privacy concerns.

As the NII evolves, many more telecommunications-mediated transactions will take place, and market forces have led to some self-regulation by telephone companies. Many have adopted privacy codes that do not allow disclosure of calling records to third parties, but other information may, at times, be disclosed. For example, some codes provide that personal information will be released to third parties only when the consumer authorizes such a release in writing, (the "opt-in" option).⁵⁸ Others only promise not to release telephone numbers or addresses if they are not published in the company's phone directory.⁵⁹ This type of policy has the unfortunate result of offering privacy only to those who pay for unlisted numbers, but not to customers who allow their numbers and addresses to be published in the phone company's directory as a public service to other telephone users.

New telephone service options continue to raise new privacy issues. Two examples are Caller ID and Automatic Number Identification (ANI). Recently, the Federal Communications Commission (FCC) approved final rules for nationwide Caller ID, which will let subscribers see the phone number of a long-distance call they receive. To protect consumer privacy, the FCC will allow callers to block their numbers from being displayed on a per-call basis and a per-line basis.⁶⁰ The California Public Utilities Commission opposed this policy, filing suit in favor of the state's automatic per-line blocking policy for all phone customers with unlisted or unpublished numbers, but a federal appeals court upheld the FCC's policy.⁶¹ With ANI, a marketing firm can immediately obtain the phone number of a caller and then obtain other specific personal data on that individual by using commercial databases. ANI personal data can easily be used to build marketing lists without a caller's knowledge or consent. No policy limits this type of activity, and most consumers are

⁵⁸ See Marc Rotenberg, "In Support of Data Protection Board in the United States," GOVERNMENT INFORMATION QUARTERLY, Vol. 8, Nov. 1, 1991, at 86.

⁵⁹ See Bell Atlantic, HANDBOOK OF COMPANY PRIVACY CODES, October 1994, reproduced from Pacific Bell's Customer Privacy Guidelines at 98.

⁶⁰ See Gautam Naik, "New FCC Rules To Let Caller ID Run Nationwide," WALL STREET JOURNAL, December 12, 1995.

⁶¹ A Federal appeals panel ruled against the California Public Utility Commission. See Evan Hendricks, editor, PRIVACY TIMES, February 15, 1996, at 4.

not aware of its existence.⁶²

4. LAWS PROTECTING THE PRIVACY OF MAIL

Privacy protections exist for both the contents of mail and the collection of certain information about mail under Federal statutory and regulatory law. Federal law protects the contents of first class domestic mail and such mail can be opened, and the contents inspected, only by authorization of the addressee, pursuant to a valid search warrant authorized by law, or by an officer or employee of the Postal Service for the sole purpose of determining an address at which the mail can be delivered.

Non-domestic mail (i.e. mail originating outside the United States) is governed by another Federal statute.⁶³ This statute permits a customs officer or other person authorized to board or search vessels to "search any . . . envelope, wherever found, in which he may have a reasonable cause to suspect there is merchandise which was imported contrary to law"

Furthermore, the Postal Service has issued regulations governing the use of the "mail cover." This is an investigative procedure whereby government officials make a record of information appearing on the exterior of first class mail, and information regarding both the exterior and contents of lower classes of mail. Under Postal Service regulations, the government's use of this investigative procedure is limited to the following purposes: to protect national security; to locate a fugitive; to obtain evidence of commission or attempted commission of a crime; to obtain evidence of a violation or attempted violation of a postal statute; or to assist in the identification of property, proceeds or assets forfeitable under law.⁶⁴ Furthermore, regulations require a written request from a law enforcement agency setting forth reasonable grounds to believe the mail cover is necessary for one of the enumerated purposes.⁶⁵

⁶² See Debra Berlyn, "Protecting Telecommunication Consumers, Privacy in the National Information Infrastructure," THE NATIONAL ASSOCIATION OF STATE UTILITY CONSUMER ADVOCATES, January 27, 1994, at 5.

⁶³ 19 U.S.C. § 482.

⁶⁴ 39 C.F.R. § 233.3.

⁶⁵ There are limited exceptions to this requirement, such as for situations involving recovery of stolen mail, dealing with damaged mail, or involving an immediate threat to persons or property. See 39 C.F.R. § 233.3(f).

D. PRIVACY IN MEDICAL RECORDS

Computerization of health care information offers opportunities to improve and streamline health care delivery, but also potentially diminishes individual privacy.⁶⁶ The challenge is to balance the privacy interest in keeping an individual's health information confidential while reaping the societal benefit derived from sharing patient records.

*WMA
LMA* Cost concerns are driving the Nation's health care delivery system to a more cost-conscious, competitive, market-based, managed care environment. Use of the NII may help provide better care for less, and better use of information technology generally can make an important contribution to reform. Existing and potential applications include telemedicine, unified electronic claims, personal health information systems, and computer-based patient records.⁶⁷ At the same time, a health care industry increasingly committed to computer networks that can collect, aggregate, and quickly and repeatedly disseminate personal medical information on a nationwide basis has raised concerns about the potential for privacy invasion and the misuse of such information.⁶⁸

1977 Report Predicts Greater Privacy Threats

As early as 1977 the Privacy Protection Study Commission recognized that the trend toward computerization of medical record information posed "new problems" from a "privacy protection viewpoint."⁶⁹ Among other things, the Commission concluded that medical records contained more information and were available to more users than ever before. Additionally, changes in the medical profession, increased population mobility, and increased demands by third parties for medical-record information had greatly diluted the control that medical care providers had once exercised over such information. The

⁶⁶ See generally, Office of Technology Assessment (OTA), PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION, 1993.

⁶⁷ See Information Infrastructure Task Force, THE NATIONAL INFORMATION INFRASTRUCTURE: AGENDA FOR ACTION, September 15, 1993, at 14-15.

⁶⁸ A recent Institute of Medicine study included among its recommendations, that the U.S. Congress enact preemptive legislation to assure the confidentiality and protection of privacy rights in person-identifiable health data. See HEALTH DATA IN THE INFORMATION AGE - USE DISCLOSURE AND PRIVACY, INSTITUTE OF MEDICINE, National Academy Press, 1994, at 190-91.

⁶⁹ See The Privacy Protection Study Commission, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, 1977, at 290.

Commission also predicted that the demand for access to such information by third party users would increase over time. The Commission observed that:

[T]he importance of medical-record information to those outside of the medical-care relationship, and their demands for access to it, will continue to grow. Moreover, owing to the rising demand for access by third parties, coupled with the expense of limiting disclosure to that which is specifically requested by the non-medical user, there appears to be no natural limit to the potential uses of medical-record information for purposes quite different from those for which it was originally collected.⁷⁰

True to the Commission's predictions, the privacy protection problems associated with the use and dissemination of medical information have only worsened. The movement toward electronic medical records has made the issue of personal health information privacy even more pressing. As a result of the linkage of computers, patient information will no longer be maintained, accessed, or even necessarily originate with a single institution, but will instead travel among many facilities further straining privacy protection.

Medical Information in the Current Networked World

Industry currently amasses and shares staggering amounts of medical information. For example, one Boston-based database, the Medical Information Bureau (MIB), serves life and disability insurance companies by maintaining extensive databanks of medical and other information on millions of Americans and Canadians.⁷¹ This information has been referred to as "the medical equivalent of a credit report".⁷² MIB is a nonprofit trade organization to which member companies are required to report the results of underwriting evaluations. The information maintained by MIB is not supposed to be used as a basis for establishing applicant eligibility but rather only to inform insurer members of the

⁷⁰ Id. at 290-91.

⁷¹ MIB maintains health records on 15 million Americans for 600 member insurance companies. See Jay Greene, "Your Medical Records - Perhaps Your Most Personal Information - Also are the Most Vulnerable to Public Scrutiny," n.8, supra.

⁷² See Melanie Hirsch, "Protecting Your Privacy - Make Sure Your Medical Records Are Accurate and Confidential," THE SYRACUSE POST-STANDARD, March 25, 1994 (1994 WL 5620138), quoting AMERICAN HEALTH MAGAZINE.

possible need for further evaluation.⁷³ MIB recently entered into an agreement with the Federal Trade Commission under which it will provide consumers a free copy of their medical information report where such information played a part in a decision to either deny coverage or charge a higher rate.

Medical records often contain highly sensitive and personal information and can reveal more about an individual than virtually any other type of record.⁷⁴ Despite the nature of this information, it is routinely shared with and viewed by third parties who are not directly involved in patient care. For example, secondary users of medical information may include educational institutions, the civil and criminal justice systems, pharmacies, life and health insurers, rehabilitation and social welfare programs, credit agencies, public health agencies, and medical and social researchers.⁷⁵ The American Medical Records Association has identified 12 categories of information seekers outside of the health care industry who have access to health care files, including employers, government agencies, credit bureaus, insurers, educational institutions, and the media.⁷⁶

⁷³ See MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA, supra, n.10 at 33.

⁷⁴ Columbia University professor and privacy expert Alan Westin has noted that information contained in medical records can have "an enormous impact on people's lives" and that such information "affects decisions on whether they are hired or fired, whether they can secure business licenses and life insurance, whether they are permitted to drive cars, whether they are placed under police surveillance or labeled a security risk, or even whether they get nominated for and elected to political office." Comments of Alan Westin, quoted in Jeffrey Rothfeder, PRIVACY FOR SALE, (Simon and Schuster 1992) at 181.

⁷⁵ See the OTA Report, supra n.66 at 2. One study found that consumers were unaware of the extent to which health insurance companies shared information concerning employees' health claims with their employers and were also unaware of the amount of information now being required in the health claims review process. See MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA, supra n.10, at 148. A 1992 WALL STREET JOURNAL article reported on the use of medical records for marketing purposes which prompted the AMA to distribute a statement warning physicians about the ethical implications of giving patient data to marketers. Id. at 198.

⁷⁶ See PRIVACY FOR SALE, supra n.74 at 180. See also Commentary, "Keeping Medical Secrets a Secret," THE CHICAGO TRIBUNE, April 5, 1996 (1996 WL 2659263) (reporting on the erosion of medical records privacy with the growth of HMOs and health

One commentator notes that although the medical and insurance industries have traditionally ensured the confidentiality of patient information, that protection is beginning to splinter due to technological possibilities and market pressures.⁷⁷

Yet there is currently no federal statute that generally protects the privacy of medical records.⁷⁸ As the OTA report observed, existing law allows development of private-sector databases and data exchanges of patient information without regulation, statutory guidance, or recourse for persons who have been wronged by misuse or abuse of the data.⁷⁹ Furthermore, the expanded use of medical records for non-treatment purposes has exacerbated the shortcomings of current legal schemes to protect privacy in patient information.⁸⁰

Consensus is emerging that traditional notions of doctor-patient confidentiality and the widely varying protection afforded under individual state laws no longer adequately protect the privacy of medical information. In its 1993 report OTA concluded that the current system fails to adequately address the

networks, the rise of commercial information companies and medical information increasingly becoming a commodity); Mike Woods & Toledo Blade, "Plug Leaks on Medical Records," HEALTH & SCIENCE, February 6, 1996 (1996 WL 3534915) (reporting on specific examples of misused medical record information appearing in a recent article in Medical Economics).

⁷⁷ MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA, supra n.11 at 195 and 200, predicting an upsurge in concerns over privacy in medical records because "[t]echnological gains in both the medical and computer worlds, buttressed by business pressures that prompt their use, are causing the environment to change much faster than the law and societal norms."

⁷⁸ Medical records held by Federal Government agencies are protected by the Privacy Act, 5 U.S.C. § 552a, but receive under that act no more protection than any other Federal record. Section 543 of the Public Health Service Act (42 U.S.C. § 290dd-2) provides protection for records of patients in federally-assisted treatment programs for alcohol or drug abuse). One survey of this area, however, noted that only about five percent of all medical records in the United States come under these limited federal statutory protections. Paul M. Schwartz, "The Protection of Privacy in Health Care Reform," 48 VAND. L. REV. 295, 315 (1995). But see n.89 infra, discussing proposed legislation.

⁷⁹ OTA Report, supra n.66, at 11.

⁸⁰ Id. at 44.

privacy issues in a computerized environment that allows for both intra- and interstate exchange of information.⁸¹ This conclusion has been echoed by Rep. Gary Condit, (D-Calif): "because health information increasingly moves from a computer in one state to a computer in another state, uniform Federal rules are needed."⁸² State privacy advocates have voiced similar concerns.⁸³

Everyone can benefit from lower health-care costs brought about by automation, but at what level does the privacy cost become too high? While there is trust in the confidentiality practices of those providing direct care, there are anxieties about increased uses of computers by direct care providers⁸⁴ and circulation of medical information beyond direct care providers to medical-information processing companies. Of particular importance in the NII environment is the concern that increased networked computer usage will allow medical information to be retrieved by people who have no medical purpose.

In response to public concerns about privacy, some health organizations and companies have responded by adopting privacy

⁸¹ Id.

⁸² Reported in Debra Beachy, "A Private Matter/Reform Raises Worry About Medical Records," HOUSTON CHRONICLE, November 21, 1993 (1993 WL 9634705).

⁸³ For example, although Wisconsin has strong medical confidentiality laws, computerized medical data flows freely to other states that may not have similar protection. This led Wisconsin privacy advocate Carole Deoppers to comment: "[i]f your prescriptions are sent electronically to some sort of company in Battle Creek, Mich., which processes HMO claims, are they protected from re-release? I don't know the answer. Federal protections are needed. You can't legislate the practices of national companies on a state level."

Likewise a Massachusetts state law gives residents of that state that right to challenge the data maintained by the Medical Information Bureau. Josh Kratka, an attorney with the Massachusetts Public Interest Research Group stated that "[i]n Massachusetts, we have a very strong privacy protection law for life and health insurance applicants" but also noted that "[n]o one else in the nation is covered by the law." Since this is a state law, the rights afforded to Massachusetts residents do not extend to anyone else.

These concerns are reported in Mary Zahn and Eldon Knoche, "States' Public Records Policies Inconsistent," MILWAUKEE SENTINEL, January 21, 1995 (1995 WL 2968305).

⁸⁴ OTA Report, *supra* n.66, at 10.

standards. Proposals for protection of personal health information generally have been based on a system of fair information principles.⁸⁵ Major model codes and statutes in this industry include the Massachusetts State Code-Insurance Information and Privacy Protection, the American Health Information Management Association's Health Information Model Legislation language, and the Uniform Health-Care Information Act of the National Conference of Commission on Uniform State Laws. As a practical matter, however, model codes and statutes have woven only a loose web of protection: they may apply to limited types of information, may not address secondary users of health information, lack enforcement powers, or simply have not been adopted (only about a dozen States have comprehensive health-care information confidentiality statutes).

Reported instances of misuses or abuses of personal health information demonstrate how difficult it can be, even when the best efforts are made, to strike an appropriate balance between cost efficiency and privacy. The following example is illustrative.

The Physician Computer Network, Inc., (PCN) is a company that is creating a nationwide computer network of doctors. PCN software links physicians to insurance companies, clinical laboratories and hospitals. The system benefits doctors and patients by saving time and money processing medical claims, receiving test results and changing medications and orders for hospitalized patients. Doctors get the service by leasing PCN computers at a discount. In exchange, PCN gets aggregated patient records, including diagnoses and treatments, which it compiles and then sells to pharmaceutical companies and insurers.⁸⁶

In response to mounting public concerns about privacy issues, PCN has implemented internal security measures and engaged a public accounting firm to certify that the PCN database remains anonymous.⁸⁷

The nation is some years away from full computer-based patient records, but most health care organizations are moving in

⁸⁵ OTA Report, *supra* n.66, at 77.

⁸⁶ *Id.* at 33-34.

⁸⁷ *See* "No Restrictions on Drug Data," LOS ANGELES TIMES May 19, 1994.

that direction. New technology will spur yet more non-traditional uses of medical data. These include computer-assisted patient assessment; joint diagnosing with desktop multimedia and a modem; and laptop-interactive-data-collecting.⁸⁸ The most recent responses to these trends are congressional bills to develop and adopt uniform national standards and national care information laws, such as the Fair Health Information Practices Act of 1995 and the Medical Records Confidentiality Act of 1995.⁸⁹ In the meantime, many issues confronting this information privacy zone remain unaddressed.

E. PRIVACY IN THE MARKETPLACE

Advancements in technology have led to the emergence of an economy that thrives on information. This new "information economy" has created a sharply increased demand for personal information and raised concerns about privacy in the marketplace. It would be impossible to discuss every aspect of this issue, since the marketplace has so many components. Instead, we have focused on selected topics that serve to frame the issues and exemplify how the government and business community balance their information needs with informational privacy values. More specifically, we focus on (1) personal financial information which is considered private by most but frequently and necessarily disclosed; (2) video rental records, which are interesting because it highlights how protecting privacy reactively leads to varying levels of privacy protections for similar types of information; and (3) direct marketing, a topic of interest to consumers and the source of many complaints to government agencies.

1. PERSONAL FINANCIAL CONDITION

Many individuals consider their financial condition a private matter and are reluctant to disclose their net worth or annual income. Yet many entities have information on our financial status, including the government (e.g., tax records), banks (e.g., loan applications), and credit reporting agencies.

⁸⁸ See Linda Holliday, "New Media Report Card: Where are We Now?" *MEDICAL MARKETING AND MEDIA*, February 1995, at 45-46.

⁸⁹ See the Fair Health Information Practices Act of 1995 (HR 435) introduced January 9, 1995, and the Medical Records Confidentiality Act of 1995 (S 1360) introduced on October 24, 1995. The latter establishes a set of rules and norms to govern the disclosure of personal health information. It would establish strong mechanisms to protect the privacy of persons with respect to personally identifiable health care information that is created or maintained as part of health treatment, diagnosis, enrollment, payment, testing, or research processes.

Frequently, the use and disclosure of this information is regulated, but information unattainable from one source may be available from another.

Tax Information held by the Federal Government

Within the government, the Internal Revenue Service (IRS) possesses the most comprehensive personal financial information. Individuals are required to report income from all sources and there are incentives (paying less tax) to itemizing certain types of deductible expenditures such as home mortgage interest, charitable contributions, and other expenses. At the same time, however, federal law protects the confidentiality of such data. More specifically, Section 6103 of Title 26 of the Internal Revenue protects the confidentiality of tax returns and return information in the possession of the Internal Revenue Service. It was enacted, as part of the Tax Reform Act of 1976, in response to Congressional and public concern about the widespread use of tax information by government agencies for purposes unrelated to tax administration.

The statute attempts to balance the Federal Government's need for the information and the citizen's right to privacy. By law, disclosure by the government may be made only as specifically provided, and unauthorized disclosure by the government subjects the offender to criminal penalties and permits the wronged party to bring a civil action for damages. The statute provides for minimum damages of \$1,000 per disclosure, and exempts the government from liability for any disclosure that was the result of a good faith but erroneous interpretation of the statute. The statute applies only to information in the possession of, or gathered by, the Internal Revenue Service; it does not include, for example, a taxpayer's retained copy of his or her tax return or financial information about a taxpayer in the possession of a third party (e.g., an accountant).

The statute covers three categories of tax material: (1) tax returns (i.e. any tax or informational return filed with the IRS); (2) return information (i.e. any financial data or information gathered by the IRS, including the taxpayer's identity, the nature, sources or amounts of his or her income, and whether the return was, is being, or will be examined or subject to other processing) and (3) taxpayer return information (i.e. return information that was furnished to the IRS by the taxpayer or his or her representative).

Finally, the statute requires the IRS to keep records of requests for disclosure and to report a summary of requests for and disclosure of returns and return information each year to Congress. Furthermore, the statute requires that Federal agencies which receive returns and return information from the IRS establish procedures to safeguard such information and to

report periodically to the IRS on those procedures. Notwithstanding this law, there have been concerns about the confidentiality of tax information. For example, it was widely reported that more than 1,300 IRS employees have been investigated for improperly accessing private taxpayer files.⁹⁰

Financial Information held by Financial Institutions

Besides the government, financial institutions also have reams of financial data on individuals. This information, too, is protected by statute; specifically, the Right to Financial Privacy Act of 1978 (RFPA).⁹¹ The impetus for enactment of the RFPA can be traced to both prior legislation and judicial decisions. In 1970 Congress passed the Bank Secrecy Act which required banks to maintain records of their customers' financial transactions. Congress imposed these recordkeeping requirements on banks because it found that such records "have a high degree of usefulness in criminal, tax, or regulatory investigations and proceedings."⁹²

In 1976, the Supreme Court held that a bank customer has no constitutionally protected right of privacy in his or her bank records because these records are the "business records of the bank."⁹³ The Court concluded that the lack of any expectation of privacy in such records was assumed by Congress when it passed the Bank Secrecy Act.⁹⁴ In 1978, Congress passed the RFPA in direct response to this decision.⁹⁵ The Act limits Federal Government access to and use of personal financial information maintained by private sector financial institutions in two ways: (1) it regulates the disclosure from the financial institution to the Federal agency in the first instance, and (2) it regulates the disclosure among government agencies where an agency has obtained records from a financial institution pursuant to the

⁹⁰ See Bill Montague and Phillip Fiorini, "Privacy Abuse Confirms the Worst Fear," USA TODAY, July 20, 1994.

⁹¹ 12 U.S.C. §§ 3401-34, Pub.L.No. 95-630 (1978).

⁹² 12 U.S.C. §1951(a).

⁹³ United States v. Miller, 425 U.S. 432 (1976).

⁹⁴ Miller, 425 U.S. at 441-442.

⁹⁵ "The title is a congressional response to the Supreme Court decision in United States v. Miller which held that a customer of a financial institution has no standing under the Constitution to contest Government access to financial records. The Court did not acknowledge the sensitive nature of these records" H. R. Rep. No. 1383, 95th Cong., 2d Sess. 34(1978), reprinted in 1978 U.S.C.C.A.N. 9273,9306.

Act.

Although the RFPA affords some measure of protection regarding government access to personal financial information, its coverage is limited in several respects. For example, although the Act requires the government to notify a customer when his/her financial records have been requested and permits the customer to challenge the government's request, it also permits delay of this notice under certain conditions.⁹⁶ Additionally, the Act provides for civil penalties and injunctive relief where financial records have been disclosed in violation of the Act but does not provide for the suppression of records so obtained. Finally, many types of disclosures are exempted from the Act's coverage (e.g. disclosure pursuant to a grand jury subpoena or in conjunction with litigation to which the government authority and the customer are parties).

The banking industry, from the consumer's perspective, is very competitive, particularly at the branch level. Unhappy with a financial institution's handling of financial records or disclosure of personal information to a marketer, a bank customer can easily establish a business relationship with another institution. This ability to "walk away," however, does not solve the more basic privacy problems of the consumer. These privacy problems are twofold: (1) the individual has little knowledge of or control over the use of his or her bank records, and (2) new information technologies are rapidly expanding the abilities of banks to collect, combine, and transmit data about customers for marketing purposes in ways inconceivable even five years ago.

Financial Services Industry Slow to Adopt New Technologies

Compared to other industries described in this paper, the financial services industry has been slow to adapt new technologies to its business practices. For instance, the banking industry resisted the introduction of Automatic Teller machine's (ATMs) and credit card magstripe technology for about 15 years.⁹⁷ This resistance may be the result of security concerns: the implementation of new technologies may create new vulnerabilities.

⁹⁶ Delay in notice may occur when there is reason to believe that notice will result in endangering life or physical safety, flight from prosecution, destruction or tampering with evidence, intimidation of potential witnesses, or will otherwise seriously jeopardize an investigation.

⁹⁷ See Sylvester Flood, "Smart Cards: U.S. Banks Take Wait and See Approach to Tomorrow's ATMs," BANK MARKETING, September 1992, at 51.

Even this industry, however, is being dramatically changed by new technology and increased customer demand for new conveniences. For example, on-line banking allows customers to pay bills, transfer money between accounts, check balances, and perform other banking transactions by computer or touch-tone phone.⁹⁸ At the same time, banks are beginning to use existing customer information more creatively, and adding demographic information to existing customer lists for targeted marketing purposes.⁹⁹ In May 1995, a Virginia mortgage bank completed what may have been the first mortgage loan originated on the Internet. The bank allows customers to download application forms, fill out the forms on a computer, and then send the document electronically.¹⁰⁰ Finally, several innovative U.S. banks are exploring the uses of smart cards, a technology that has been more widely accepted in Europe.

If smart card or prepayment card technology become as popular as ATMs, major privacy concerns may be raised. Smart cards have the potential to contain a customer's entire credit, purchase, and medical history, along with any other data that can be stored on a microchip. In fact, it is primarily privacy concerns that are slowing the acceptance by the industry of this technology.¹⁰¹

The move from traditional banking services into other areas such as database marketing presents new privacy concerns for the industry. For example, card-issuing banks have access to direct-marketer customer information as part of their billing procedures. Privacy advocates suggest that while the bank may own the customer information collected before extending credit, it should not claim ownership of the data generated between the direct marketer and the customer. The use of that data by the bank is an invasion of privacy.¹⁰²

Database marketing has likewise brought banks into business

⁹⁸ See Kristin Davis and Scott Nelson, "Safe Travel on the Info Superhighway: Measures to Protect Individuals' Privacy when Paying Bills Electronically," *KIPLINGER'S PERSONAL FINANCE MAGAZINE*, January 1994.

⁹⁹ *MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA*, supra n.10 at 27 and 80-83.

¹⁰⁰ See Marianne Hyriahos, Kathleen Day, and Jonathan D. Glater, "Netting a Loan," *THE WASHINGTON POST*, May 5, 1995.

¹⁰¹ See Flood, supra n.97.

¹⁰² See Thomas J. Little, "Privacy vs. Data Use: A Matter of Survival," *CATALOG AGE*, at 103.

relationships with buyers and sellers of personal information who do not have the historical confidentiality practices of financial institutions and who currently are essentially unregulated in their use of personal data (see the previous discussion of direct marketing). It is the dramatic fall in the price of computer storage that has made it possible for businesses to accumulate and maintain large quantities of data about their customers. For 10-cents a name, middlemen offer extensive data on most U.S. families.¹⁰³

Although, as discussed above, financial institutions possess detailed information about the financial lives and transactions of their customers, such records are not well protected by privacy laws. Moreover, unlike some other industries examined in this paper, banking has not established an over-arching set of recommended privacy principles. Indeed, as of June 1996, neither of the two main trade associations for the banking industry had established privacy guidelines for banks to follow.¹⁰⁴ Some individual financial institutions, however, have adopted privacy codes. BankAmerica's code describes the dilemma in the following manner:

Privacy is not a new concept in banking. By law and custom, it is recognized throughout the world that the relationship between a bank and its customer is confidential. The proliferation of computers has made the adherence to this concept of privacy more complex. Specifically, the public's concern has centered on the difficulty an individual can have in discovering and controlling what data will be collected about him or her, challenging the accuracy of the data, and determining who will have access to that data and for what purpose.¹⁰⁵

Other banks have developed internal policies on handling and

¹⁰³ See Saul Hansell, "Getting to Know You," INSTITUTIONAL INVESTORS, June 1991, at 71.

¹⁰⁴ See Robert E. Kearney, "Keep Your Hands Off My Data," BANK MARKETING, May 1995, at 19. These two trade associations are the American Bankers Association and its affiliate, the Bank Marketing Association. However, the 850 member Consumer Bankers Association is developing a privacy code that will require members to establish internal privacy standards. See John N. Frank, The Brouhaha over Privacy, CREDIT CARD MANAGEMENT, May 1996 at 32.

¹⁰⁵ See Bell Atlantic, HANDBOOK OF PRIVACY CODES, October 1994, reproduced from BankAmerica Corporation Privacy Code, at 48 (emphasis added).

disseminating customer information. Examples of such policies include: not releasing account numbers along with personal financial information furnished to credit bureaus, and entering into a confidentiality agreement that precludes a third party service provider, such as a supplier of credit life insurance, from using customers' names for any other purpose.¹⁰⁶

Fortunately, companies which have been leaders in exploiting information about their customers also have been leaders in adopting formal privacy policies.¹⁰⁷ These policies generally restrict disclosure of data to those with a "business need" to see it, and often offer consumers the ability to "opt out" of receiving promotional mail. Unfortunately, many of these principles give consumers little say about what it means to have their personal data treated carefully, and the opt-out programs do not limit the information that financial companies collect about their customers or purchase from outside sources.¹⁰⁸ Also, there are hundreds of list brokers with whom banks deal who are far removed from the public eye and are never subject to consumer pressure to adhere to financial institution or privacy standards.

In the information age, the lax protection of privileged financial information among banks, credit bureaus, and software manufacturers, especially when combined with other types of information such as demographic profiles, could result in the misuse or abuse of personal information. As banks merge and become more electronically oriented, the potential for a veritable explosion in privacy complaints intensifies. Yet, as noted above, there are few laws and privacy principles in place. Whether privacy standards in the banking industry will keep pace with the industry's adoption of new information technologies remains to be seen. As we approach the end of the 20th century, financial institutions are walking a tightrope strung between the conflicting goals of providing services in an increasingly competitive marketplace through increased reliance on electronic communications to customers, and respecting and protecting

¹⁰⁶ See Cynthia Graham, "Banks Must Address Consumer Privacy Concerns," *PRIVACY & AMERICAN BUSINESS*, March 1995, at 23.

¹⁰⁷ See Hansell, *supra* n.103 at 22.

¹⁰⁸ See *MANAGING PRIVACY - INFORMATION TECHNOLOGY AND CORPORATE AMERICA*, *supra* n.10 at 17-27, noting that although banks are some of the most highly regulated institutions in the U.S., most Federal banking regulation has focused on issues related to solvency and to fairness in lending.

consumers' privacy.¹⁰⁹ According to one industry spokesperson, confidentiality of customer information has been the missing link for providing on-line transactions.¹¹⁰ In order for "cyberbanking" to become accepted practice, either market forces or regulation will have to limit the use of personal information in ways that unacceptably compromise informational privacy.

Financial Information held by the Credit Reporting Industry

Banks are not the only repository of financial information; credit bureaus have large files on individuals. Indeed, the nation's three major bureaus keep files on nearly 90 percent of American adults, that is, anyone who buys something on credit.¹¹¹ The use of this information is, to some degree, limited by the Fair Credit Reporting Act (FCRA).¹¹² Originally enacted in 1970, its purpose is to ensure that consumer reporting agencies adopt reasonable procedures to meet the legitimate needs for consumer credit information in a manner that is fair to the consumer with respect to the confidentiality, accuracy, relevancy, and proper use of such information.¹¹³ With two exceptions,¹¹⁴ the legislation has remained substantially unchanged.

The Act provides some protection to consumers with respect to the information maintained about them by consumer reporting agencies. For example, it places a time limit of seven years on the adverse information that an agency may include in its consumer reports. There are, however, two exceptions: there is a 10 year limit for bankruptcies and no time limit for certain

¹⁰⁹ See Evan Hendricks, Financial Privacy, CREDIT WORLD, November/December 1994, at 26.

¹¹⁰ See editorial, "Financial Services Can Now Be Offered On Internet," BANK MARKETING, May 1995, at 82.

¹¹¹ See "What Price Privacy?" CONSUMER REPORTS, May 1991, at 356.

¹¹² 15 U.S.C. § 1681, et seq.

¹¹³ 15 U.S.C. § 1681(b)

¹¹⁴ These are a reduced time period for including information on bankruptcies in credit reports from 14 to 10 years in 1978, and the Consumer Credit Reporting Act which was passed in 1992. Although the Consumer Credit Reporting Act (CCRA) provides additional protection to consumers with respect to errors in their credit reports, the CCRA makes no changes to the original statute with respect to who may have access to credit reports (i.e., it leaves intact the "permissible business purpose" exemption).

transactions involving substantial amounts of money. The Act also prohibits the production of "investigative consumer reports," which are reports on a consumer's character and reputation based solely on interviews, without disclosure to the consumer and other safeguards. Furthermore, whenever a consumer is denied credit for personal, family, or household purposes, or is denied employment, and the denial is based on information in a consumer report, the entity that received and used the report is required to notify the consumer and identify the consumer reporting agency in question.

The FCRA also imposes requirements on consumer reporting agencies, such as ensuring compliance with the Act; providing consumers with information from their files; establishing procedures for dealing with disputes about the completeness or accuracy of information maintained in their files, and taking special precautions, when reporting public record information, to ensure the completeness and accuracy of that information or, in the alternative, to notify the consumer that such information is being reported.¹¹⁵ Finally, the Act places some restrictions on the dissemination of credit information to third parties. For example, it provides that a consumer reporting agency may disseminate a report on a consumer only pursuant to a subpoena or court order; with the consumer's consent; or for use in connection with one of several enumerated purposes.

FCRA Permits Anyone with a "Permissible Business Purpose" Access to Credit Reports

The Act, however, permits anyone with a "permissible business purpose" to purchase credit reports. Senator Proxmire, an original proponent of the FCRA, had sought to limit the disclosure of confidential credit information only to those third parties, such as banks and other credit grantors, who needed access to this information to make credit granting decisions.¹¹⁶ The FCRA as passed, however, included the "permissible purpose language." This broad exemption to the disclosure limitations of the Act has raised privacy concerns among some commentators. For example, one commentator has noted that just one of the "big three" credit reporting agencies sells 500,000 records each day and that credit reporting agencies share information not only with banks and other credit grantors but also with numerous other third parties such as employers, landlords, private investigators, and others.¹¹⁷

Other commentators have criticized the FCRA for vague

¹¹⁵ See 15 U.S.C. §§ 1681(c)-(k).

¹¹⁶ See PRIVACY FOR SALE, supra n.74, at 56-57.

¹¹⁷ Id. at 38 and 33 respectively.

drafting, poor enforcement, obsolescence in the face of technological change, and lack of consumer education.¹¹⁸ Additionally, commentators have pointed out that only limited transactions are protected. For example, the FCRA does not cover exchanges of information involving business transactions, only those involving personal, "consumer"-oriented matters.¹¹⁹ In addition, since the FCRA only applies to the items specifically enumerated in the statute, certain categories that arguably should be included, such as credit reports in connection with insurance claims, are excluded from coverage.¹²⁰

The credit reporting industry is dominated by three giant credit bureaus -- TRW Information Services (TRW), Equifax, and TransUnion. The credit bureaus sell credit reports to credit grantors so that they can assess a history of payments, how much credit already is available to the consumer, and other indices of the potential to repay a credit grant. Businesses that grant credit, such as banks, retail stores, and credit card issuers, report the credit history of their customers to these credit bureaus. Other than the Federal Government, the credit reporting industry maintains the largest repositories of information about Americans.¹²¹ For the consumer, the credit reporting industry does not provide competitive options. Credit reports about an individual are often maintained by more than one of the big three bureaus, and the consumer will only know which bureau possesses what information if he or she makes the effort to acquire his or her credit records. Within the industry, however, there is a great deal of competition between the large credit bureaus for the business of credit grantors.

Industry Adopts Voluntary Privacy Policies

Although formal regulation has not changed since the passage of the FCRA more than twenty-five years ago, the industry has adopted some voluntary privacy standards and mechanisms to correct erroneous personal information. For example, in response to the demand for fair standards for the treatment of credit information, two of the three credit bureaus have developed privacy codes. TransUnion has not publicized a privacy code.

¹¹⁸ See statements of CHERYL B. PRESTON, "Honor Among Bankers: Ethics in the Exchange of Commercial Credit Information and the Protection of Customer Interests", 40 KANSAS L. REV. 943, 995 n.31 (1992).

¹¹⁹ Id. at 947.

¹²⁰ See Elwin Griffith, *The Quest for Fair Credit Reporting and Equal Credit Opportunity in Consumer Transactions*, 25 U. MEMPHIS L. REV. 37, 46 (1994).

¹²¹ See *PRIVACY FOR SALE*, *supra* n.74 at 32.

TRW maintains credit information on more than 190 million credit-active consumers in the U.S. and claims to process and file 43 million pieces of information each day.¹²² TRW has observed that: "Computers and telecommunications have made it easier to use information to benefit others. But it also is easier to harm others through information uses."¹²³ In an effort to respond to their own concerns, the company has established what it calls a values approach to guide decisions on how to use information.¹²⁴

Equifax has 200 million credit reports in its files. Equifax first created and published a code of fair information practices in the 1980's, and has recently updated that code.¹²⁵ Also, to better understand consumer privacy attitudes, Equifax has fielded numerous initiatives such as annual national surveys of consumer attitudes about privacy. Furthermore, in 1990, Equifax responded to mounting consumer and privacy concerns by establishing a toll-free number that consumers could call to order credit reports, obtain advice, and correct inaccuracies.¹²⁶

During recent years the credit reporting industry has come under increasing consumer attack on consumer issues. For example, mounting consumer complaints about inaccuracies in credit reports and difficulties encountered in attempting to correct such errors led to the passage of the Consumer Credit Reporting Act in 1992. In response to ongoing public complaints about the credit reporting industry, the industry's trade association, the Associated Credit Bureaus (ACB), and consumer representatives in 1992 agreed on a set of standards for Federal legislation to improve the FCRA. Although this Federal legislation was never enacted, in January 1993, the ACB board of directors implemented as mandatory member policy initiatives the amendments to the FCRA it had supported. Receiving major consideration were privacy, accuracy, and consumer relations issues.¹²⁷ Additionally the industry has recently acted to establish standards and procedures for the automation of consumer

¹²² See TRW Home Page at <http://www.trw.com/iss/iss.html>.

¹²³ Id.

¹²⁴ See TRW, FAIR INFORMATION VALUES, July 1994.

¹²⁵ See Bell Atlantic, HANDBOOK OF COMPANY PRIVACY CODES, October 1994, at 34-43.

¹²⁶ PRIVACY FOR SALE, *supra* n.74 at 58.

¹²⁷ See Barry Connelly, "Credit Bureaus Adopt Initiatives in the Absence of a New Law," CREDIT WORLD, July/August 1993, at 7.

dispute verification¹²⁸ and has created a specialized electronic mail network to speed resolution of consumer complaints about inaccurate personal information.¹²⁹ Also, in 1992 Equifax agreed to a consumer credit information gathering and dissemination codes in cooperation with 18 states. TRW had reached a similar agreement in 1991.¹³⁰

As positive as these efforts may be, credit bureaus continue to be criticized regarding privacy issues and database errors and have agreed to settlements with both Federal and state regulators to correct the problems.¹³¹ Regulators and lawmakers are continuing their efforts to impose some restrictions on data gathering and on the manipulation and dissemination of commercially held data.¹³² The bulk of these continuing complaints against the credit reporting industry fall into two categories: (1) damaging mistakes in the credit report, and (2) release of names to marketers and others who do not meet the "permissible use" requirement under the FCRA.

Reverse Appending and Prescreening Generate Privacy Concerns

Newer techniques such as "reverse appending" and "prescreening" also are being used by the industry to increase efficiency and cut costs. Use of these techniques, however, generate many privacy concerns. Some commentators have directed particularly harsh criticism at "prescreening," a process whereby a credit reporting agency compiles or edits lists of consumers who meet specific criteria and then sells the lists to a credit

¹²⁸ See Kenneth Solomon, "Consumer Dispute Verification," CREDIT WORLD, March/April 1994, at 28.

¹²⁹ See, for example, Mitch Betts, "Credit Industry Employs E-Mail Address to Address Dispute Resolution Woes," COMPUTERWORLD, April 4, 1994, at 61. Also, Gary Belsky, "Junk Mailers Lose One in the Privacy Battles," MONEY, December 1994, at 46.

¹³⁰ See unsigned article, "Equifax Agrees to Info Gathering Standards," INFORMATION INDUSTRY BULLETIN, July 2, 1992, at 5.

¹³¹ See Mitch Betts, "FTC Targets Credit Bureau Mailing Lists," COMPUTERWORLD, January 18, 1993, at 20; unsigned article, "Equifax Settles Charges by FTC," DIRECT MARKETING, April 1995, at 7.

¹³² See Trudie Bushey, "Are Access and Use of Public and Private Information at Risk?" CREDIT WORLD, March/April 1995, at 6.

grantor or marketer.¹³³ The lists are used to target consumers for credit and other products and services. Criteria may include such personal information as age, income, marital status, and place of residence. This practice is arguably inconsistent with the Privacy Principles' "Fairness Principle" regarding the need to give consideration to the "individual's expectations regarding the use of the information."

Advances in computer technology that allow both the targeting of marketing lists and the combining of databases in easy-to-use formats will continue to challenge the credit reporting industry to establish and/or implement fair standards that apply to all uses and users of the vast quantities of data they maintain regarding the credit histories of U.S. citizens.

2. VIDEO RENTAL RECORD PRIVACY

The Video Privacy Protection Act,¹³⁴ passed in 1988, is a classic example of the reactive nature of U.S. privacy legislation. Prior to passage of the Act, video rental records were not protected by Federal law and a person could walk into a video store and obtain a list of all movies rented by a particular customer without that customer's permission. It was only after a list of then Supreme Court nominee Robert Bork's video rental records was published in a Washington, D.C., newspaper that Congress became interested in the privacy concerns associated with such records and passed protective legislation.¹³⁵

Outraged at this attack on Judge Bork's privacy, Congress determined that Americans should be free to watch rented films in the privacy of their own homes without fear that their video rental records could be disclosed to the public. Therefore,

¹³³ One commentator has expressed the view that "prescreening is not a 'permissible purpose' under the FCRA in that the disclosure is not 'in connection with a transaction involving the consumer'" and that "the Act should be amended to require that an individual's actual consent be obtained, by either the reporter or the third party, before information can be disclosed." See Amendments to the Fair Credit Reporting Act: Hearing Before the Subcommittee on Consumer Affairs and Finance of the House Committee on Banking, Finance, and Urban Affairs, 101st Cong., 2d Sess. 122 (1990) (statement of Janlori Goldman)

¹³⁴ 18 U.S.C. § 2710.

¹³⁵ As explained by the Los Angeles Times, "the [law]...was written [by Congress] after a weekly Washington newspaper obtained and published the video rental records of Bork." Los ANGELES TIMES, October 20, 1988 (1988 WL 2197371).

under this act, a video store that knowingly releases a customer's rental information or video purchases is liable for damages to that customer. There are logical exceptions to this rule, however. For example, such information can be released with the customer's consent, and a law enforcement agency can obtain this information pursuant to a search warrant, court order, or grand jury subpoena.

Different Protections for Cable Movie Records

Of course, individuals also rent movies on pay-per-view cable and, to the extent an individual's choices in video selection is a private matter, the law should protect that information consistently. But cable movies are subject to a different standard. Under the Cable Communications Policy Act (CCPA), enacted to establish a cohesive national cable communications policy and to set guidelines for the cable television industry, cable subscriber information may be disclosed to a government entity only pursuant to a court order,¹³⁶ a higher standard than a grand jury subpoena.

Although juxtaposing video stores and cable companies highlights a significant discrepancy regarding the same information (video rental records), cross-sector inconsistencies exist as well. For example, the CCPA protects personally identifiable information, including lists of names and addresses on which the subscriber is included.¹³⁷ The rationale:

Cable systems, particularly those with a 'two-way' capability, have an enormous capacity to collect and store personally identifiable information about each cable subscriber...subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions.¹³⁸

Although this statement is undeniably true, telephone billing records may similarly reveal much about an individual (e.g., phone calls to a psychiatrist's office on a regular basis). Yet phone records are subject to grand jury subpoenas; cable records only obtainable with a court order. With telecommunications deregulation and the possibility of cable companies offer phone service and phone companies offering television service, these inconsistencies will become more

¹³⁶ Title 47 U.S.C. §551(h).

¹³⁷ 47 U.S.C. § 521, et seq.

¹³⁸ H.R. Rep. No. 934, 98th Cong., 2nd Sess. 29 (1984), U.S.Code Cong. & Admin. News 1984, pp. 4655, 4666.

glaring.

Of course, turning over records to the government is only one concern; the other is how the records are used by the industry itself. Therefore, the Act restricts the ways in which cable companies may collect, retain, and disclose personally-identifiable subscriber information, and requires industry to inform consumers of their rights and available remedies. The Act does not prohibit marketing all personal information collected by the local cable operator (this would protect privacy without considering the legitimate commercial uses for the information), but rather allows cable operators to disclose the names and addresses of subscribers as part of a mailing list if they have provided the opportunity for subscribers to prohibit such disclosures and the mailing lists do not reveal the nature or extent of subscribers' uses of services.¹³⁹

Although this policy balances the cable companies' desire to use information with an individual's possible privacy interest, it is interesting to note that the Cable Act and its privacy provisions apply only to cable-based communications--not to direct broadcast satellites and wireless transmissions. Thus, whether there are restrictions on the use of data, and whether the consumer has the right to opt-out, is technology specific rather than dependent upon the type of information at issue.

3. DIRECT MARKETING

The direct marketing industry has been a prime beneficiary of the technological advances in information processing. According to one industry commentator "the database revolution is the most significant recent arrival in the direct marketing industry...."¹⁴⁰ New technologies process, manipulate, combine, and exchange personal data in unprecedented quantities both quickly and economically, thus allowing industry to target goods and services to consumers in new ways. Implementation of the NII will create even more opportunities to combine and exchange personal data as well as provide additional avenues for communication with prospective customers.

The Line Between Improved Customer Service and Invasion of the Customer's Privacy

Direct marketing accounts for \$350 billion dollars in sales

¹³⁹ See Ronald L. Plessner, Testimony before the Privacy Working Group of the National Information Infrastructure Task Force, January 27, 1994.

¹⁴⁰ See Gary Levin, "Database Draws Fevered Interest," ADVERTISING AGE, June 8, 1992, at 31.

annually.¹⁴¹ About half the people in the U.S. now buy by mail.¹⁴² The benefit of target marketing to the industry and consumers is the increased likelihood that catalogs and other promotional material will end up in the hands of consumers who are genuinely interested in these materials. In other words, customer service can be improved by target marketing and shoppers are offered extended shopping hours and immediate delivery as well.¹⁴³

But the proliferation of databases and lists of consumers that are produced from them also raise privacy implications. By collecting information regarding consumer preferences and purchases, marketers ultimately have possession of a person's name, address, buying habits, and other individual social and economic data. Individuals currently have no legal right to be notified of data stored about them, who has the data, who has organized it into lists, and with whom such personal data is shared. Also, there is no legal prohibition against using information gathered for one purpose for an incompatible purpose.

This situation has served to focus attention on the fine line between customer service and invasion of the customer's privacy. One recurring problem is that individuals who feel they are harmed by a direct marketer's use of personal information still lack control over the use of this information.¹⁴⁴ Additionally, consumers frequently complain about receipt of large amounts of unsolicited mail and mail from complete strangers with highly personal information.¹⁴⁵ Indeed, the leading consumer complaints about the direct marketing industry concern unsolicited mail and telephone calls.¹⁴⁶ The Direct Marketing Association (DMA), with a membership of some 3,500

¹⁴¹ Comments of Direct Marketing Association spokeswoman Lorna Christi, reported in THE LOS ANGELES TIMES, May 18, 1994.

¹⁴² See Judith Waldrop, "The Business of Privacy," in AMERICAN DEMOGRAPHICS, October 1994, at 47.

¹⁴³ Comments of Deborah Zizmore, Direct Marketing Association's New York Headquarters, report in LOS ANGELES TIMES, May 18, 1994, supra n.12.

¹⁴⁴ See unsigned article, "Study Says Consumers Lack Control of Personal Info," DIRECT MARKETING, April 1994, at 9, citing Privacy Rights Clearinghouse, FIRST ANNUAL REPORT.

¹⁴⁵ See generally Denison Hatch, "Privacy: How Much Data do We Really Need?" TARGET MARKETING, February 1994.

¹⁴⁶ Privacy Rights Clearing House, SECOND ANNUAL REPORT, January 1995, at 23.

manufacturers, wholesalers, and retailers, is the largest national trade association serving this industry.¹⁴⁷ The DMA readily admits to receiving many calls from consumers involving flyers from stores never shopped in, catalogs from mail order companies never ordered from, and banks and card companies never communicated with.¹⁴⁸ This problem appears to stem from the use of personal information by third parties, such as database compilers, credit reporters, or credit-card issuing banks.

Some commentators have argued that consumers should be notified of the lists they are placed on and should have input into how personal information about them is used.¹⁴⁹ Most recently the National Telecommunications and Information Administration (NTIA), in its report on privacy issues associated with the telecommunications sector, recommended notice to and consent by the customer in the collection and use of TRPI (telecommunications-related personal information).¹⁵⁰ Nonetheless, privacy concerns about direct marketing practices have produced little legislative regulation and this state of affairs provides an opportunity to examine one sectoral response to privacy concerns in an industry that is very competitive, largely unregulated in its use of personal information, and concerned about public opinion.

Industry Adopts Voluntary Codes and Standards

For years, the direct marketing industry has grappled with maintaining the balance between the consumer's right to privacy and the direct marketer's use of consumer data.¹⁵¹ The DMA has taken affirmative steps to address the privacy concerns of its customers through reliance on its own codes and standards. The DMA has established an ethical code and guidelines for self-regulatory action, and may refer members found in violation of

¹⁴⁷ See generally, Direct Marketing Association, *PRIVACY: THE KEY ISSUE OF THE 90'S A DIRECT MARKETER'S GUIDE TO EFFECTIVE SELF-REGULATORY ACTION IN THE USE OF INFORMATION*, 1993, at 21.

¹⁴⁸ See Henry Hoke, editorial, *DIRECT MARKETING*, October 1944, at 82.

¹⁴⁹ For example, Evan Hendricks, publisher of *PRIVACY TIMES* has argued for a law requiring firms to tell consumers their name is being added to a list and to give consumers a chance to say no. Reported in *BOSTON GLOBE*, September 6, 1993, supra n.12.

¹⁵⁰ *PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION*, NATIONAL TELECOMMUNICATIONS INFORMATION AGENCY, October 1995.

¹⁵¹ See Tim Little, "Privacy vs. Data Use: A Matter of Survival," *CATALOG AGE*, May 1992, at 103.

the code to its ethics group or can suspend membership in the association.¹⁵² The DMA has sponsored a Mail Preference Service (MPS) and a Telephone Preference Service (TPS) to handle, on a national level, unsolicited junk mail and telemarketing. Both are designed to assist consumers in decreasing the amount of national commercial and non-profit mail and national commercial telephone calls they receive at home.¹⁵³ MPS mail volume is growing at a rate of about a million names per year.¹⁵⁴ Beyond the MPS and TPS, the DMA recommends that individual companies give consumers an opportunity to opt out of the exchange of marketing data through in-house suppression programs and disclosure notices.¹⁵⁵

The DMA encourages its members to adopt its several corporate information programs to respond to consumer privacy sensitivities. Adoption of and adherence to the DMA's recommended privacy practices is voluntary for its members. Furthermore, not all direct mailers are members of the DMA. Nonetheless, many direct mailers have adopted individual privacy codes tailored to the DMA's recommendations. One example is TRW, one of the largest credit bureaus¹⁵⁶. As part of its direct marketing product overview TRW answers the question "What are fair information practices?" in the following way:

- o Fair information practices are codes of conduct for using information.
- o One such set of guidelines is the fair information checklist developed by the Direct Marketing Association, an industry trade group. Association members follow the checklist to prevent any use of information that might harm consumers...TRW, a DMA member, obeys these industry guidelines...¹⁵⁷

While acknowledging the usefulness of self-regulation, some

¹⁵² See LOS ANGELES TIMES, May 18, 1994, supra n.12.

¹⁵³ See n.147, supra at 21, 23.

¹⁵⁴ See n.148 supra.

¹⁵⁵ See n.147 supra at 9.

¹⁵⁶ TRW, Inc. reported on February 9, 1996, that it plans to sell its Information Systems and Services unit that keeps credit records to two private investment companies. Reported February 9, 1996, by The Associated Press.

¹⁵⁷ <http://www.trw.com/iss/tmspo.html#question20>. See also TRW, FAIR INFORMATION VALUES, July 1994.

commentators have expressed concern about whether self-regulation adequately safeguards privacy. Others wonder whether the DMA does (or can) effectively enforce its fair information codes. For example, the fact that adherence to DMA's recommended privacy practices is voluntary has led one commentator to state that "[t]he only rules which limit the use of the most personal information by direct marketers are the rules which the marketers voluntarily choose to follow."¹⁵⁸ Concerns have also been raised that there is no guarantee that information brokers will adhere to DMA's recommended practices.¹⁵⁹ Appeals to direct marketers to opt-out may work if the marketer abides by the DMA fair information standards. Consumers can have their names placed in the MPS and TPS name removal files, as explained above, but how would a consumer know who had compiled a list sold to a direct marketer or had supplied the personal data on the list? Tracking the original source of TRPI will grow progressively more complex with the maturing of the NII. Indeed recent problems encountered by Metromail, illustrate these concerns.

Metromail, a subsidiary of R.H. Donnelley and Sons Company, maintains mail-order and telephone information on 93 million households, broken down by consumer tastes and demographics. This information includes a Families with Children List containing 20 million addresses and a Teenagers File with five million names. Metromail has recently been involved in a number of privacy related controversies; for example, the release of information concerning 5000 Los Angeles households, including the addresses and ages of children, to a television reporter using the name "Richard Allen Davis" (Davis was recently convicted in San Jose for the kidnap and murder of 12 year old Polly

¹⁵⁸ Statement of Mary J. Culnan, Associate Professor, Georgetown University School of Business, reported in LOS ANGELES TIMES, May 18, 1994, supra n.12.

¹⁵⁹ "It costs pennies to draw a list of names from a computer data base and start assembling a marketable profile that can be sold for as much as \$200 per thousand names. There is only one other industry that operates on that kind of markup, and that's illicit drugs. So long as the list business is that profitable, it is going to spawn greed, and privacy invasion and corruption, just as illicit drugs do." Comments of Denison Hatch before a luncheon of industry executives, reported in NEWSDAY, July 21, 1993, supra n.12. See also, Shelly Reese, Future Shop Customers "Draw Line on Privacy Issue," CINCINNATI ENQUIRER, May 24, 1994 (reporting on the fact that there are currently about 10,000 lists which get sold and rented to other retailers usually at a rate of about \$50 or \$55 per 1,000 names).

Klaas).¹⁶⁰ Metromail is also currently being sued by an Ohio woman who received sexually offensive mail from a Texas prison inmate who was provided access to a consumer questionnaire she had filled out. The questionnaire had originally been sent to Metromail who in turn passed it on to a contractor for further processing. The contractor, in turn, passed this information on to the Wynne prison unit in Huntsville, Texas for prisoners to process the questionnaires. The woman asserts that this use of her personal information was done without either her knowledge or consent.¹⁶¹

Conflicts such as these will continue to stalk the direct marketing industry as indicated by complaints to the Federal Trade Commission. Furthermore, the NII will ease and make more efficient the compiling and exchange of ever more targeted lists. Nonetheless, the direct marketing industry as represented by the DMA has done much to balance privacy and personal-data-use interests. Whether or not competitive forces in the industry will encourage even more agreement on and adoption of fair information practices, as well as provide meaningful sanctions, will determine whether the volume of consumer complaints spirals upward or downward and whether public policy in regard to personal information use may need to be more formalized.

IV. OPTIONS FOR PROTECTING INFORMATIONAL PRIVACY ON THE NII

As we have seen, the United States has no legally defined, comprehensive right to informational privacy that spans both the public and private sectors. Implicit in the discussions throughout this Paper, however, is the recognition that there is a societal importance to informational privacy which is relevant to both sectors.

Thus, we turn to the core question: could we do better in balancing the needs of government, commerce, and individuals, keeping in mind both the interest in the free flow of information and the protection of informational privacy? In attempting to answer this question, this section explores three different approaches to privacy protection in the information age.

First, we could maintain the status quo, with the current mix of policy and legislative initiatives.

Second, we could maintain the status quo but enhance

¹⁶⁰ See Evan Hendricks, editor, *PRIVACY TIMES*, Vol 16. No.10, May 17, 1996.

¹⁶¹ See Robert Ellis Smith, editor, *PRIVACY JOURNAL*, Vol.22, No.7, May 1996.

existing efforts with new government led initiatives. For example, a new privacy initiative could be implemented to highlight privacy's importance and develop consumer awareness, thereby increasing consumer demand for privacy and helping to make it a bargained for market commodity.

Third, the Federal Government could create a centralized Privacy Entity (PE) to address privacy issues.

We address each issue in turn.

A. MAINTAINING THE STATUS QUO

This section addresses the possibility of taking no new action with respect to informational privacy, instead choosing to maintain the status quo. As set forth throughout this Report, it is clear that some measures have been taken, by both the public and private sectors, to deal with privacy issues and to respond to growing public concerns with new threats to privacy. It is equally clear, however, that privacy is currently dealt with in a segmented and piecemeal fashion and that responses often occur only after a particular privacy issue has become problematic.

As with all the other factors considered in this paper, retention of the status quo is also subject to differing opinions based on viewpoint. For example, maintaining the status quo could be viewed as providing both the public and private sectors the maximum flexibility in addressing privacy issues, thereby not unduly restraining either sector. The viewpoint that market forces can be relied upon exclusively to correct any and all problems that may arise and that the Privacy Principles will readily be embraced promptly by both the public and private sectors also would support maintaining the status quo. On the other hand, maintaining the status quo could be viewed as taking an "ostrich like" approach, palpably insufficient to address the diverse and complex privacy issues that continue to arise in an increasingly networked environment. Discussed below are several considerations that may be helpful in evaluating the feasibility of this option.

The Public Sector

In the public sector, certain agencies are currently active in the privacy arena. For example, in October 1995, The National Telecommunications and Information Administration (NTIA) published a Whitepaper on Safeguarding Telecommunications Related Personal Information and has followed up this Report with letters to approximately 45 telecommunication companies and associations concerning their privacy practices and the implementation of NTIA's recommendations. NTIA has advised that in the next few months it will be meeting with private sector representatives after which it will make a determination whether additional government action through either legislation or

regulation is warranted.¹⁶² NTIA has also advised that it recently coordinated a discussion of the EU Privacy Directive Public among representatives of the EU, the private sector, and other Federal agencies.

Likewise, the Federal Trade Commission (FTC) has recently assumed a key role in the privacy arena and indeed has been identified in *PRIVACY AND AMERICAN BUSINESS* as the most privacy active agency.¹⁶³ For example, the FTC recently entered into an agreement with the Medical Information Bureau (MIB), the nation's largest repository of medical and other personal information serving the insurance industry. Under this agreement, when information provided to an insurer by MIB played a part in the decision to deny coverage or to charge a higher rate, insurance companies must disclose that fact and provide MIB's name and address. In these circumstances, individuals are entitled to receive a free copy of their medical information report, on file with MIB, in order to verify that all information is correct.¹⁶⁴

The Office of Consumer Affairs (OCA) has been active in educating the public about a variety of privacy issues and was instrumental in establishing the Privacy Working Group of the IITF. In addition, OCA has worked with industry to preserve consumers' privacy and control over the use of their personal

¹⁶² In the late 1970's, under the Carter administration, the NTIA was tasked with coordinating the legislative work of that administration's privacy initiative, developing an international privacy initiative (in conjunction with the State Department), monitoring non-Federal information practices, and studying the growth of information technology on privacy. In the early 1980s NTIA was involved, in conjunction with the State Department, in negotiating the establishment of privacy guidelines within the OECD and worked with U.S. companies to encourage endorsement of these guidelines. During that time, NTIA had fifteen staff handling privacy issues but NTIA then experienced reductions in force and its staff dwindled.

¹⁶³ *PRIVACY AND AMERICAN BUSINESS*, Vol.2, No.2, August 1995, at pp 4-5. See also, Jay Greene, "Eluding Their Gaze//The Way to Protect Personal Info is to Leave No Trace but Remember - The Rules Aren't In Your Favor," *THE ORANGE COUNTY REGISTER*, April 25, 1996 (1996 WL 7024132) (reporting that in privacy matters "[t]he FTC, which regulates unfair and deceptive trade practices, has been perhaps the most aggressive federal agency in reining in credit bureaus, medical-records gatherers and others").

¹⁶⁴ See, "Consumer Rights Expanded Under reporting Rule Effective in October," *FTC NEWS* September 29, 1995.

data while encouraging both growth and innovation in the use of telecommunications and information management technology.¹⁶⁵ The Internal Revenue Service has also taken steps to address privacy issues within its own agency. In June 1993, it established the Office of Privacy Advocate with a staff of 12.

Despite the laudable efforts of these agencies, some privacy concerns are not within any particular agency's purview. For example, although some medical records held by Federal Governmental entities are currently protected by the Privacy Act and by other very narrowly drawn statutes, only about 5% of all medical records in the United States come under these limited federal statutory protections.¹⁶⁶ Additionally, a recent article reported on the absence of privacy protection for e-mails and provided several examples, among them that of a California supercomputing company who had retrieved the e-mails of three company executives, two of whom had recently resigned, in order to learn more about the relationship of the two departing executives who had joined a rival research group.¹⁶⁷

Furthermore, other areas of privacy straddle one or more agencies. For example, the Department of Health and Human Services and the Department of Energy jointly considered the privacy implications of the ability to acquire genetic information about individuals. In the international arena, several agencies have been involved with privacy issues arising from transborder data flows. For example, NTIA participated in the development of OECD privacy guidelines in the early 1980s, the Justice Department is currently involved with OECD efforts related to the security of data contained in computer systems in the global information infrastructure,¹⁶⁸ and the Office of Consumer Affairs also has been an active participant at the OECD

¹⁶⁵ See Statement of Bernice Friedlander, Acting Director OCA, before the House Appropriations Committee Subcommittee on VA-HUD-Independent Agencies, April 18, 1996 (1996 WL 5511468).

¹⁶⁶ See Paul M. Schwartz, The Protection of Privacy in Health Care Reform, 48 VAND.L.REV. 295, 315 (1995).

¹⁶⁷ See, David Folkenflik, "Electronic Mail Writers have Practically no Privacy, and Their Lack of Legal Protection is Opening the Way for Punishment in Courts and Workplaces," THE BALTIMORE SUN, April 27, 1996.

¹⁶⁸ Congress has recently introduced legislation (S.982) drafted by the Justice Department, that would more broadly protect the confidentiality of data. This legislation was based, in concept, on the OECD Guidelines for the Security of Information Systems.

on consumer privacy issues.¹⁶⁹ In each of these cases, as presently required, the State Department has been involved.

Different information privacy issues raise different concerns and priorities, and require different types of expertise to deal with adequately. Currently several Federal agencies are addressing a variety of privacy issues in different ways. For example, some agencies such as the FTC have regulatory authority while others, such as OCA, serve an advisory and educational function. Some agencies' sphere of influence extends to the private sector (e.g. NTIA and FTC) while other agencies' privacy oversight extends only to the public sector (e.g. OMB's oversight of the Privacy Act).

Under the status quo, however, no agency currently involved with privacy issues has privacy as even its primary, much less its only mission. This means that privacy must compete, in terms of budget and manpower, with the other responsibilities that these agencies are charged with. There is currently in place no one focal point for privacy in the public sector that would (a) permit agencies to maintain their current areas of privacy responsibility while (b) facilitating the work of those agencies who are currently active in the privacy arena, and encouraging a more comprehensive and coordinated privacy response across the board by the public sector.

The Private Sector

As discussed throughout this Report, some segments of the private sector have taken affirmative steps to address privacy issues arising in the modern networked environment. For example, as noted previously, the Direct Marketing Association (DMA) has established guidelines and an ethical code for its members in the use of personal information about consumers. Additionally, the DMA is revising its policy guidelines to reflect the realities of electronic marketing, including spamming, and several independent organizations now offer on-line dispute resolution services to deal with, inter alia, privacy problems. Yet, unsolicited mail and telephone calls continue to be a major source of consumer dissatisfaction with direct marketers (supra n.146). Likewise, while both TRW and Equifax have adopted voluntary privacy standards (supra pp. 42-42), the credit reporting industry continues to be a leading source of complaints to the Federal Trade Commission.¹⁷⁰

¹⁶⁹ For example, the OCA leads the U.S. Delegation to the OECD Committee on Consumer Policy.

¹⁷⁰ Reported in Ann Merrill, "Credit Bureaus Continue to be Leading Source of Complaint about Privacy," MINNEAPOLIS-ST. PAUL STAR TRIBUNE, February 11, 1996.

Furthermore, as with legislative responses, changes in private sector privacy practices often occur in response to some precipitating event. For example, in the early 1990s, mounting consumer dissatisfaction, adverse media coverage and highly publicized lawsuits preceded changes in how the credit reporting industry dealt with consumer access to credit reports and ultimately led to amendments to the Fair Credit Reporting Act.¹⁷¹ Most recently, in the wake of mounting consumer criticism and an agreement reached with the FTC, consumers now have greater access to personal information maintained by the Medical Information Bureau (supra p.53).

The Privacy Principles were published less than a year ago, and even if the status quo is maintained, it is reasonable to expect that in time some segments of both the public and private sectors will voluntarily bring their practices into line with these principles. It is equally reasonable to expect, however, that other segments will require some precipitating event or outside impetus to do so. Under the status quo, there is in place no one focal point to aid in (a) identifying the myriad privacy issues increasingly facing the private sector in today's networked environment; (b) encouraging dialog among and between the private, public and international sectors on privacy issues; and (c) facilitating and coordinating timely and effective responses. A recent article in *PRIVACY AND AMERICAN BUSINESS* appears to indicate that such a focal point would be welcomed.¹⁷²

The States

Under the status quo, in the absence of overriding federal legislation, privacy concerns are often addressed by the 50 individual states either through state laws or state constitutional protections. This is an exceedingly difficult task in the context of a networked environment where personal data transfers occur continuously across state lines.¹⁷³ Although some states have been at the forefront in the privacy

¹⁷¹ See e.g. *PRIVACY FOR SALE*, supra n.74 at 58-62.

¹⁷² See n.182 supra.

¹⁷³ The proliferation of computerized databanks has ignited an explosion in the number of lists that individuals' names appear on. Upwards of five billion records exist in the United States containing personal information about individuals and this information about each person is moved from one computer to another on the average of five times per day. *PRIVACY FOR SALE*, supra n.74 at 90 and 17.

arena,¹⁷⁴ widely varying levels of privacy protection among the various states creates difficulties for businesses operating in several states and affords individuals inconsistent levels of protection based on the accident of their geographical location. State privacy advocates have recognized the need for a unified response to privacy issues in the current environment.¹⁷⁵

Finally, although maintaining the status quo offers the obvious benefit of requiring no immediate expenditure of funds, this benefit may prove to be ephemeral. In the absence of any focal point to address the myriad privacy issues arising in an increasingly networked environment, these initial savings may well be outweighed in the long run by the cost of such things as lawsuits, increased regulatory action, fallout from adverse publicity, new legislation and decreased business opportunities in the international marketplace.

In conclusion, as discussed throughout this Report, the history of privacy protection in the United States has generally been one of piece-meal responses, narrowly tailored to deal with only a limited type of information maintained by a particular sector. Perhaps the biggest down side to maintaining the status quo is to ensure that the same reactive and piece-meal approach that has predominated the U.S. privacy response in both the public and private sectors will continue. Whether this uncoordinated and segmented means of dealing with privacy is workable in an increasingly networked world remains an open question.

B. ENHANCED GOVERNMENT ROLE UNDER THE STATUS QUO

If the current methods of protecting privacy is inadequate, can we transform current privacy protections into something more orderly and predictable without creating a new entity? This section explores the possibility of enhancing the current government approach so that it can operate more cohesively and

¹⁷⁴ For example, California has a state constitutional right to privacy as well as statutory privacy protection. In 1994, a California court ruled against an individual who sought a county's entire municipal court information database because of the privacy implications inherent in the aggregate nature of the personal information contained in that database [*Westbrook v. County of Los Angeles*, 27 Cal. App.4th 175, 32 Cal. Rptr. 2d 382 (July 1994)]. The court based its decision on a governing state statute and on the state's constitution. In a state without these statutory and constitutional protections, however, the decision may well have gone the other way.

¹⁷⁵ See n.83 supra.

pro-actively. The question is whether such an "enhanced" approach can overcome charges that the traditional sectoral approach cannot address privacy concerns comprehensively and consistently, and before conduct has become unacceptably invasive.

In past years, the government and private industry have become more active with respect to privacy. Congress is debating several statutory solutions to problems associated with medical information, the collection of data from and about children, communications privacy, and consumer privacy issues arising, or expected to arise, in connection with electronic commerce. On June 4 and 5, 1996, the Federal Trade Commission's Bureau of Consumer Protection held a public workshop on Consumer Privacy on the Global Information Infrastructure, which provided an opportunity for consumer groups, privacy advocates, members of the online industry and others to explore privacy issues posed by the collection of personal information in electronic commerce. Several organizations demonstrated technology that consumers can, or will soon be able to, use to protect their personal information online. Trade associations representing the advertising, marketing, and online service industries announced new or revised privacy codes and consumer education programs for the information age. Several workshop sessions were devoted to examining the collection of data from and about children online. Similarly, NTIA recently issued a White Paper on telecommunications privacy, and is now meeting with telecommunications providers to determine if they are adhering to the privacy principles outlined in the report. NTIA, with the Department of State, is also holding discussion with the European Union on the EU Directive.

Why are such initiatives under way now? There are probably a number of explanations for this phenomenon. First, now that the ease with which the NII will allow data to be collected, distributed, analyzed has become clearer, government and consumers are more aware of the electronic medium's data gathering capabilities. As a result, there is now greater government and consumer demand for privacy enhancing products and policies. This can be viewed as an example of the free market in operation. In the Information Age, privacy may become a market commodity. Given adequate levels of consumer and government awareness, demand for privacy protection could continue to increase and a robust, competitive market for privacy protection could develop. Under this scenario, the market itself could serve the same function as a privacy entity.

Government could facilitate the development of this privacy market in three distinct ways. First, the Government could get its own house in order by ensuring that government data collection remains consistent with the Privacy Principles in the face of changing technology. The Office of Management and Budget

is responsible for enforcing the Privacy Act, for example, and might profitably review that statute along with federal agency adherence to it in light of the NII Privacy Principles.¹⁷⁶ OMB could report its findings and recommend legislation, regulation or executive orders to solve any problems it discovers. This kind of review could provide a model for private sectors to undertake similar audits.

Second, government could play a larger role in consumer and business education. Agencies with responsibility for privacy could act as "bully pulpits" to raise consumer and business awareness of the issue. Consumer education is likely to raise demand for information privacy protection to its optimal level. Business education is also necessary to introduce technology entrepreneurs to consumer protection theory, which in turn could help industry anticipate the privacy implications of a new product. The expense associated with consumer and business education would be minimized if the industries that will benefit most directly from increased consumer confidence in the NII were to accept some responsibility for this program.

Third, government could enhance self-regulation by exploring enforcement deficiencies with industry. This would address the most oft-heard complaints about self-regulation; that industry codes of conduct are praiseworthy, but largely unenforceable. Industry often responds that competition law in the United States limits their enforcement efforts. More work is needed to understand whether, and how, other values, including competition, undermine enforcement activities. Government and industry might then work together to resolve any such conflicts pro-competitively.

All of these roles will require, of course, the substantive and sectoral expertise of individual government agencies.

While much can be done in this way, the downsides of such an approach are self-evident. First, it may be viewed by some as little more than the status quo approach in a new package. For example, the increased legislative activity, while appropriate, is reactive; the privacy of medical records has been an issue for years. Moreover, the steps the government could reasonably take to protect privacy (i.e., getting its own house in order, playing a larger role in consumer and business education, and enhancing self-regulation by exploring enforcement deficiencies with industry) are all steps that could have been taken years ago.

Second, this is still a sectoral approach without any overarching vision for how privacy can best be protected. This

¹⁷⁶ Additionally, OMB could be provided with additional staffing to enforce the Act more effectively.

could well be viewed as a continuation of piecemeal legislative efforts and sectoral approaches that will continue to lead to inconsistent privacy protections, and may frequently fail to anticipate future developments in a comprehensive, thoughtful way. Indeed a centralized focal point for privacy could actually facilitate enhanced agency efforts by permitting agencies to maintain their current spheres of responsibility while assisting these agencies in indentifying and responding to privacy issues in a comprehensive and coordinated manner.

Last, although market forces undoubtedly have played and will continue to play a critical role in protecting privacy, relying too heavily on market forces is arguably a mistake, especially in cases where the consumer is not in an equal bargaining position with industry. For example, as noted above, consumers who have unlisted numbers must pay to protect their privacy. Certainly those consumers who must choose between paying for privacy or foregoing phone service are not finding their privacy protected by free market forces. Additionally, free market forces have no applicability when there is no relationship between the consumer and the private sector entity collecting or using personal information. For example, individuals cannot choose which credit bureau will maintain their credit report. And few consumers have even heard of the Medical Information Bureau. Neither education nor market forces are of much help here--a person suffering from cardiac arrest needs immediate medical care; there is not time to negotiate with the ambulance attendant over whether the hospital's records will be referred to the MIB.

C. CREATION OF A PRIVACY ENTITY

Could the creation of a Privacy Entity serve to better protect the privacy of NII participants? In attempting to answer this question, this Section discusses those factors that would bear upon the determination to establish some type of privacy focused entity.

- o Part 1 considers the functions that such an entity could perform, including the upside and downside of these functions.
- o Part 2 discusses the placement of such an entity, provides examples of various models upon which the entity could be patterned, and discusses the upside and downside of the various models.
- o Part 3 addresses the various spheres of influence that the entity could have.
- o Part 4 comments briefly on such an entity's composition.

Finally, Appendix A sets forth a tabular representation of the discussions of the functions and placements in Parts B and C of this section and offers some sample decisional trees.

1. Functions

- a. *The Regulatory Function*

A privacy entity could regulate government, the private sector, or both. Perhaps the most obvious characteristic of a regulatory function is "clout." A regulatory function would enable a privacy entity to mandate specific actions and to ensure compliance with its mandates through, for example, enforcement proceedings. Furthermore, an entity with a regulatory function may well be able to effect desired changes more quickly than an entity whose function is advisory only and who would, therefore, have to build a consensus over a longer period of time.

It should be noted, however, that the regulatory function does not exist as an absolute positive or negative. Indeed whether it is perceived as a benefit or a detriment is usually a function of individual viewpoint. For example, while privacy advocates may consider a regulatory function beneficial and necessary, some members of the business community may view such a function as unnecessary, preferring instead to effect constructive change through an advisory function or some other means. Others may view a regulatory function as potentially harmful to the evolving NII.

Regardless of individual viewpoint, certain considerations may be helpful in evaluating the regulatory function. For example, it is useful to consider a potential regulatory function in the context of what is to be regulated. In the privacy universe, this could translate into extremely broad regulatory power. Information privacy covers an increasingly complex and diverse range of issues that arise in both the public and private sectors. As such, a privacy entity tasked with regulating the entire privacy universe would regulate, among other things, banks (because of financial records), private mail services (because they may possess transactional data), the telecommunications industry (because of electronic surveillance), the medical community (because of medical records), and catalog companies (because of targeted mail and transactional data). The costs of such a regulatory scheme could be significant. Furthermore, the very broad regulatory scope in the privacy context may well raise concerns that, in this time of deregulation, the Federal Government is seeking to create a new agency whose regulatory powers reach into every aspect of American life.

Finally, a regulatory function raises additional questions regarding the adoption and enforcement of the regulatory scheme. For example, before regulations can be adopted, a fact-finding

process is generally required to determine the seriousness of any particular problem and what remedies will be effective. In order to carry out this fact-finding process, a privacy entity would need some method of compelling agencies, businesses, and individuals to provide information (most likely by subpoena power). This in turn raises ancillary questions such as the cost of complying with subpoenas, and whether the privacy entity would have independent litigating authority to compel compliance. Then there is the costs and efforts associated with the regulations' enforcement.

b. The Advisory Function

Alternatively, a privacy entity could perform an advisory function in the public sector, the private sector or both. Such an advisory role could be confined to coordinating domestic policy or could extend to the international arena. An advisory function can be viewed as being at the opposite end of the spectrum from a regulatory function and, like the regulatory function, whether it is perceived as a benefit or a detriment is largely a matter of individual viewpoint. For example, those who want to see quick action on privacy issues may criticize an advisory function as not being sufficiently effective. Others may believe that having privacy experts lending advice would significantly balance and promote important interests without burdening society with the costs and intrusiveness generally associated with a regulatory function.

Again, regardless of individual perspective, certain considerations may be helpful in evaluating this function. For example, an advisory function may well be viewed, by both the public and private sectors, as less intrusive than a regulatory function, and therefore may be accepted more readily by both sectors. Additionally, the scope of the advisory role also may have an impact on its effectiveness. If the advisory role is structured to offer advice across a broad spectrum in both the public and private sectors, it is less likely to be viewed as a spokesperson for any particular interest group. An example of such broad based advice would be assisting both government agencies and the private sector in complying with the IITF PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION as an aid to ensuring even implementation of a uniform set of information use standards and thereby increasing public trust in the NII.

Finally, a privacy entity which advises but does not regulate would be unable to either compel or prevent particular action (*i.e.* it could recommend certain action but would have no means to enforce its recommendation). As a practical matter, it may not be able to bring about specific desired changes as rapidly as an entity with a regulatory function could, since it would have to build a consensus and influence change by persuasion over time rather than by mandate.

c. The Educational and Research Functions

A privacy entity could also engage in a variety of educational and research functions, including funding research to assist policy makers and the public. For example, it could issue periodic reports on the state of privacy that would address important privacy issues and suggest solutions. Most privacy organizations in other countries prepare such reports. For example, the French National Commission on Informatics and Freedoms submits an annual report to the President and to Parliament. The Data Protection Commission in Germany publishes an annual report to the national legislature, and the British Data Protection Registrar reports annually to the House of Commons. This function could also include establishing and maintaining a library devoted to privacy related materials.

On the upside, educating the public on privacy issues may have the salutary effect of diminishing or avoiding privacy violations and helping to ensure that those who ignore privacy rights suffer repercussion through market forces, rather than necessitating legislation and lawsuits to address abuses. This can also help both consumers and users to develop realistic expectations concerning data use and privacy. Additionally, educating individuals about what types of redress are available when information is misused and educating data users on how to respond to consumer complaints effectively can assist business in retaining good will while resolving difficult problems relating to information use and privacy. To assist in this effort, a privacy entity could maintain a library that includes not just resources readily available from other sources (e.g., Federal and state statutes and legislative histories), but also sectoral policies and guidelines; individual company policies; articles on different aspects of personal information privacy; and materials regarding foreign laws, policies, and practices could result in this repository becoming the leading source of privacy information worldwide. All materials maintained at this library could be made available to the public both at the library and through on-line access.

On the downside, the educational and research functions would require additional funding and personnel resources. Depending on the budget that would realistically be available to such an entity, resources may be better used to perform one or more other functions.

d. The Ombudsman Function

An ombudsman function could give a privacy entity broad authority to intercede on behalf of citizens with Federal, state, and local governments, and the private sector. It could provide a central source for citizens to contact about privacy concerns.

As such, an ombudsman function might actually forestall or decrease the use of the courts to resolve privacy related disputes. Likewise, an ombudsman could serve as the U.S. representative in international privacy disputes, ever more likely due to the international nature of existing networks and the expected increase in transborder data flows.

There are, however, certain significant considerations that may be useful in evaluating this function. First, in a country with the population of the United States, the number of anticipated complaints would be extremely high, and the ombudsman role could quickly overtake all the resources of a privacy entity (even if the entity could choose which disputes to handle, the mere processing of the requests would likely be time consuming and costly). Second, it would have to be decided whether, in fulfilling an ombudsman function, the entity would simply advise parties on how to resolve their dispute, or be the actual decision maker (as in binding arbitration).

e. The Coordination and Representational Functions

A privacy entity could undertake coordination and representation functions if it were tasked with (1) coordinating domestic privacy policy, (2) serving as the chief spokesperson on domestic privacy issues, and (3) representing the United States internationally. Regardless of individual viewpoint on the merits of such a tasking, the following discussion may be helpful in evaluating these functions.

In the area of domestic coordination and representation, a privacy entity could officially be tasked with ensuring that government agencies protect privacy in consistent ways. For example, many Federal agencies need to collect debts, an activity that can often be facilitated by collating records revealing an individual's location and assets. Such collection activities also affect privacy, however, and a coordinating entity could ensure that agencies collect debts in compatible ways that reflect an appropriate respect for privacy. On the other hand, a centralized approach may limit the ability of agencies to address such problems in unique and innovative ways.

The entity might also represent the President's privacy views both domestically and internationally. This could be viewed as a downside because, if given such broad powers, the entity would have to assume responsibilities currently handled by several agencies (e.g., Commerce, State, Justice), and be an expert not just on privacy, but on the many underlying substantive issues which, in turn, give rise to privacy issues. Such a tasking may well raise concerns whether one entity could assume the work of so many agencies, and have such a broad base of knowledge.

However, if the entity were given a *coordinating* role internationally, this might help alleviate a current problem encountered by countries and international organizations: the lack of a single U.S. point of contact on privacy matters. Indeed, a privacy entity could be influential in the international arena without having a formal international representation function. For example, it could serve as the United States' coordinator to the international community on privacy issues, without having an international representation function. This would serve the salutary goal of having one centralized location to which foreign governments could look when dealing with information privacy issues. Currently, if a foreign office wants to understand United States privacy policies, it must query literally dozens of Federal agencies. A single point of contact could well be viewed as facilitating international relations in this area. It could also serve to affirm the United States' commitment to privacy issues. This role would be limited to coordinating and advising only--it would not extend to negotiating formal privacy treaties with foreign governments, which is the province of the State Department. Finally, with respect to international representation, foreign policy is traditionally the responsibility of the President (often with the advice and consent of Congress). Thus, giving a privacy entity this function would dictate its placement within the Executive Branch.

2. Placement

a. *Placement of the Entity Within the Executive Branch - Executive Agency or Federal Spokesperson*

One possibility is to place a privacy entity within the Executive Branch by creating either an Executive Branch Agency or a Federal Spokesperson or "Czar." Such executive branch entities can be created either through Congressional action or by Executive Order. For example, the United States Office of Consumer Affairs (OCA) was created by Executive Order. The National Telecommunications and Information Administration (NTIA), which was originally created by Executive Order to serve as the Executive Branch agency responsible for advising the President on telecommunications and information policies, subsequently had these responsibilities codified by the NTIA Organization Act of 1992. The Office of Government Ethics, which was originally part of the Office of Personnel Management, became a separate agency under the Ethics in Government Act of 1978, as amended (5 U.S.C. app. 410). Both the Drug Czar and the AIDS Czar were created by Executive Order.

Executive Branch Agency

On the upside, the ability to create an entity by Executive Order, as an alternative to legislative action, could

significantly decrease the amount of time required to get such an entity "up and running," since Congressional efforts at creating such an entity have not succeeded. Also on the plus side is the potentially wide range of functions such an entity could perform. For example, depending on its mandate, an Executive Branch Agency could perform regulatory, advisory, educational/research and ombudsman functions. Moreover, its influence on privacy matters could extend to both the public and private sectors, and to both the domestic and international arenas.¹⁷⁷ This is not to suggest an endorsement of any particular function or sphere of influence but merely to acknowledge the broad scope of activities that such an entity could engage in.

On the downside, an executive branch entity may be viewed by some as partisan. For example, the highest ranking officials of an Executive Branch Agency are normally appointed by and serve at the President's pleasure. Such an agency is also, however, accountable to the President, Congress and the public. As such, its agenda may well be subject to considerable review and external pressure. Additionally, executive branch agencies tend to be larger and therefore more expensive than, for example, a Federal Spokesperson office which is discussed immediately below.

Finally, since an Executive Branch Agency potentially has available to it a wide range of functions and, since the public and business community affected by such an entity often hold widely divergent views, the same functions that may be viewed as a plus by some may be seen as a negative by others. For example, some may see a benefit in educational and research activities while others may view such functions as an unnecessary drain on limited resources. Likewise, some may hail a regulatory function as a long overdue necessity while others will find it unduly intrusive. As such, careful thought would need to be given to what specific functions the entity would have. The analysis of the various functions set forth above, as well as the comments and opinions received from members of the public and private sectors in response to this Paper, can be helpful in evaluating the option of an executive branch agency.

Federal Spokesperson or "Czar"

On the upside, as with an Executive Branch Agency, the fact that it can be created solely by Executive Order can

¹⁷⁷ For example, although OCA, NTIA and OGE can all perform advisory and educational functions, only OGE performs a regulatory function. Likewise, although all three agencies are active in the domestic arena, only OCA and NTIA operate in the international arena. Finally, the OCA focuses on both the public and private sectors, the NTIA focuses primarily on the private sector, and the OGE focuses on the public sector.

significantly decrease the time for it to become operational. Furthermore, although a Federal Spokesperson or "Czar" would not have the same range of functions that an Executive Branch Agency,¹⁷⁸ he/she could still be quite influential in protecting privacy interests. For example, although Federal Spokespersons primarily influence the public sector, their "bully pulpit" role can extend to the private sector and into the international arena as well. A Spokesperson or "Czar" is established to serve as a focal point for Government action in an area of serious public concern. As such, a privacy "Czar" could be viewed as well positioned to achieve uniformity of approach among disparate agencies and to provide a single point of contact in the United States for dealing with the European Union and individual foreign countries. Finally, unlike Executive Branch agencies, which as noted above tend to be large and expensive, a Spokesperson or "Czar" would likely require a much smaller and less costly office.

On the down side, Spokespersons can be eliminated or moved to less visible positions as easily as they can be created. Since Spokespersons lack de jure authority, their influence is dependent upon their ability to speak for the President. Indeed, it is a Spokesperson's connections with the President, and the exercise of actual or apparent Presidential influence, which is the source of the Spokesperson's influence or power. Finally, from a budget perspective, if the Spokesperson is located in the Executive Office of the President and funded from that budget, this can present continuing funding problems. On the other hand, if the Spokesperson is located elsewhere, his/her connection with the President is weakened. Finally, as in the case of an Executive Branch Agency, a Spokesperson or "Czar" is also appointed by and accountable to the President and serves at the President's pleasure. Thus it likewise may be viewed by some as a tool of Administration policy. Furthermore, its agenda may also be subject to considerable review and influence, although a Spokesperson's stature may permit him/her to set his/her own agenda to some extent.

b. Placement of the Entity Outside the Executive Branch - Independent Regulatory Commission

Independent regulatory commissions are established by Congress to attempt to respond to complex issues of national importance. For example, the Federal Trade Commission was established in 1914, through the Federal Trade Commission Act, codified at 15 U.S.C. §§ 41-58, to prevent unfair methods of

¹⁷⁸ Normally a Federal Spokesperson or "Czar" does not regulate, conduct research or function in an ombudsman capacity. However, he/she could still perform advisory and educational functions.

competition and unfair or deceptive business practices. Over the years Congress has passed additional laws, such as the Magnuson-Moss Act of 1975, to give FTC greater authority to police anticompetitive practices. Likewise, the Commission on Civil Rights was originally created by the Civil Rights Act of 1957, as amended, and reestablished by the U.S. Commission on Civil Rights Act of 1983, 97 Stat. 1301, codified at 42 U.S.C. 1975. Independent regulatory commissions carry out critical regulatory functions through the application of regulatory statutes, rules and regulations. Their sphere of influence may extend to both the public and private sectors as well as to the domestic and international arenas.¹⁷⁹

On the upside, the independence of this type of entity may give it greater credibility with the public. For example, it is generally headed by three or more commissioners who are appointed by the President for *fixed terms*. It operates as a quasi-legislative, quasi-judicial organization and is almost independent of Congressional oversight (its adjudications, however, are subject to judicial appeal, and its budget requires Congressional reauthorization and appropriation). This degree of separateness and independence gives it much greater flexibility to set its own agenda. Also on the plus side is the potentially wide range of powers of such an entity. For example, it can use its judicial authority to develop policy on a case-by-case basis, having the power to subpoena both witnesses and documents and to hold fact-finding hearings. It can promulgate regulations and ensure their enforcement. In addition to its adjudicatory and regulatory powers, it can also foster voluntary compliance with relevant law by way of staff advice, advisory opinions and the issuance of guidelines delineating legal requirements in regard to practices.

On the downside, this level of independence may be perceived by some as not sufficiently accountable. The public can often lack a practical mechanism through which to communicate views. Additionally, its potentially broad regulatory powers could raise concerns that in this time of deregulation, the Federal Government is creating a new entity whose regulatory powers reach into so many aspects of American life. There may also be concerns that such an entity would tend to engage in numerous case-by-case adjudications as a method of formulating policy rather than resorting to less formal procedures such as dialogues and exchanges of information with industry. Finally, independent

¹⁷⁹ For example, the FTC works with the European Commission of the European Union, and with the Organization for Economic Cooperation and Development, and the Asia-Pacific Economic Conference to promote competition policies that can be followed by all participating states. *See Anticipating the 21st Century*, FEDERAL TRADE COMMISSION, Spring, 1996 at 11.

commissions tend to be quite large and expensive.

c. Placement of the Entity Within an Already Existing Agency

A privacy entity could also be placed within an already existing agency. On the upside, as noted above, a number of Federal agencies are already involved with a variety of privacy issues both in-house and in interactions with the private and the international communities. As such, these agencies already have some knowledge of and experience in dealing with certain kinds of privacy issues. Additionally, it may well be easier and less costly to create an entity within an already existing organizational framework.

Although not either a specific upside or downside to placing the entity within an already existing agency, certain considerations may be helpful in evaluating this option. First, privacy today has become a complicated matter and is expected to become increasingly so with the continued expansion of the NII. Different areas of information privacy raise very different concerns and priorities. They also require different types of expertise to address them in a meaningful manner. The agencies currently involved with privacy issues are dealing with specific areas of privacy that these agencies are uniquely qualified to handle (e.g. privacy issues arising in consumer transactions, in telecommunications, in law enforcement, in government records, etc.). None of these agencies' areas of responsibility extends to the entire universe of privacy. Second, none of these agencies is dedicated exclusively to or focused exclusively on privacy and indeed, their primary mission is something other than privacy. As such, privacy must of necessity compete with other agency priorities for funding and personnel. The competing responsibilities of the larger organization could well dilute the effectiveness of a privacy entity placed within the larger structure.

d. Placement of the Entity as an Advisory Committee

A Federal Advisory Committee can be created to provide advice in a particular area. It can only be created by Executive Order and usually consists of a number of Presidentially appointed members with expertise in the specific area that the Committee was created to address. For example, the National Security Telecommunications Advisory Committee (NSTAC) was created by the President in 1982 to advise him on matters regarding National Security/Emergency Preparedness telecommunications (NS/EP). Its membership consists of 30 presidentially appointed industry leaders representing major carriers, information service providers, manufacturers, electronics firm, and aerospace firms. The NSTAC's principal

working body, the Industry Executive Committee, supervises subgroups that address specific issues in more detail. The NSTAC works in conjunction with the National Communications System (NCS). The NCS is comprised of 23 Federal departments and agencies and is the government equivalent of the NSTAC. The NCS has a small permanent staff that functions as the Executive Secretariat for the NSTAC. The two organizations can coordinate their activities to ensure both public and private sector coverage.

On the upside, the independence of such an entity may give it greater credibility with the public. For example, although the Committee members are appointed by and provide advice to the President, they are not political appointees and are highly independent. Additionally, based on their composition and expertise, such committees sphere of influence can extend to both the public and private sectors. This type of entity can be quite effective in facilitating dialog among interested parties. For example, the NSTAC has been extremely effective addressing telecommunications security issues by opening lines of communication between government and industry.¹⁸⁰ Finally, costs are generally quite limited. For example, the cost of the NSTAC/NCS is manageable because the NSTAC members donate their time, and the NCS has only a small permanent staff (with member agencies also providing representatives and detailees).

On the downside, such an entity generally works well because it focuses on a narrow range of issues (for example, in the case of NSTAC--national security/emergency preparedness telecommunications). Additionally the members often share common interests and philosophies (in the case of NSTAC, protecting the telecommunications network). This uniformity may be difficult to translate to a broad area representing widely divergent views, such as privacy.

Finally, this type of entity traditionally performs a narrow range of functions, being limited to advisory, educational and research functions. Whether or not this limited range of functions is a plus or a downside will ultimately turn on the specific functions a privacy entity will be expected to perform.

3. Sphere of Influence

Ultimately, the functions assigned to an entity and its placement will affect its sphere of influence. However, generally speaking, an entity could have influence in the public

¹⁸⁰ The NSTAC and NCS publish regular reports, recommend legislative fixes, collect information about network incidents and coordinate joint government-industry responses to telecommunications issues.

and/or private sectors and the domestic and/or international arenas. As a practical matter, the broader the entity's sphere of influence, the greater its potential impact on privacy matters. At the same time, however, a broader sphere of influence would require more staffing/funding and the day-to-day administration would be more complicated. Additionally, depending on the precise functions and placement of the entity, certain spheres of influence would be problematic (e.g. a non-executive branch cannot be responsible for foreign policy).

Regardless of what decision is ultimately reached with respect to such an entity's appropriate sphere of influence, the following discussion of the role such an entity can play in each sphere may be helpful in determining which spheres the entity's influence should extend to.

Federal agencies today are dealing with numerous privacy issues, from records management and the Privacy Act, to the inherent tension between effective law enforcement and individual privacy concerns, to the privacy implications of genetic testing. Additionally, public opinion polls reveal that more people today are worried about privacy invasions by government agencies than by private sector businesses (see n.17 supra). As such, a privacy entity would have a role to play in addressing the diverse privacy issues faced by the public sector.

Likewise, advancements in computer technology coupled with the integration of telecommunications and data processing have resulted in a tremendous increase in the acquisition of personal information by the private sector. As noted in the discussions in Sections II and III, although the private sector has taken steps to protect personal privacy, some corporate privacy policies remain inadequate or suffer from a policy/practice gap. Thus, a privacy entity also would have a role to play in facilitating the identification and resolution of the myriad privacy issues faced by the private sector in a networked environment.

Finally, an increasingly networked world will result in increased transborder data flows. Additionally, because many European countries now have data protection laws and the European Union has approved a directive regarding information privacy, the growing disparity between U.S. and European information privacy protection may pose difficulties for U.S. business interests.¹⁸¹ For this reason, a privacy entity may well have a role to play in addressing privacy issues arising in a global

¹⁸¹ See n.21 supra and accompanying text.

environment.¹⁸²

4. Composition

Finally, a brief note about the entity's composition. The broad range of privacy issues that exist and could be addressed by a privacy entity suggests that careful thought be given to its composition. An entity whose members bring existing expertise to bear on the many and complex privacy issues facing an increasingly networked world, and whose expertise will be heightened through immersion in the field and through contact with other domestic and foreign privacy experts, may be best equipped to deal effectively with these issues. This is not to suggest that those addressing privacy issues today have not been successful but rather to acknowledge that privacy is very much its own specialty and will continue to raise ever more diverse and complicated issues in a globally networked world.

V. CONCLUSION

Currently, privacy is protected in the United States through a combination of statutes, regulations, and voluntary codes of conduct that apply to the public and private sector. Yet today personal information is being collected at a rate and to a degree unthinkable even twenty years ago, and much of that information can be legally sold, shared, exchanged and disseminated without notice to or input by the individual.

Legislative responses are often reactive and piecemeal in nature. For example, video rental records are protected under federal law, but personal medical information is not. Additionally, laws that were adequate when enacted may have become obsolete or ineffective with advances in technology. Thus, video rental records held by cable companies receive a different level of protection than video rental records maintained by video rental stores.

Policy responses are also flawed. Although industry codes of conduct are becoming more sensitive to privacy problems, such codes are not uniformly adopted by all sectors, or by all

¹⁸² For example, a recent issue of *PRIVACY AND AMERICAN BUSINESS* reported that a privacy protection office "could have positive aspects helpful in encouraging, but not dictating, privacy supportive conduct: by assisting the business community in convincing the European Community that the United States can meet EC "adequacy" standards; and by helping to create privacy policies in federal governmental agencies that are appropriate and predictable." See *PRIVACY AND AMERICAN BUSINESS*, Vol 2, No.2, March/April 1996 at p 20.

companies within a sector. Additionally, they are viewed by many as unenforceable.

The three most logical options available to policy makers are to maintain the status quo, increase current efforts (status quo plus), or create a privacy entity to address privacy issues. Each of these options has advantages and disadvantages with regard to cost and effectiveness, all of which must be carefully considered if we are to protect privacy efficiently and effectively in the information age.

APPENDIX A

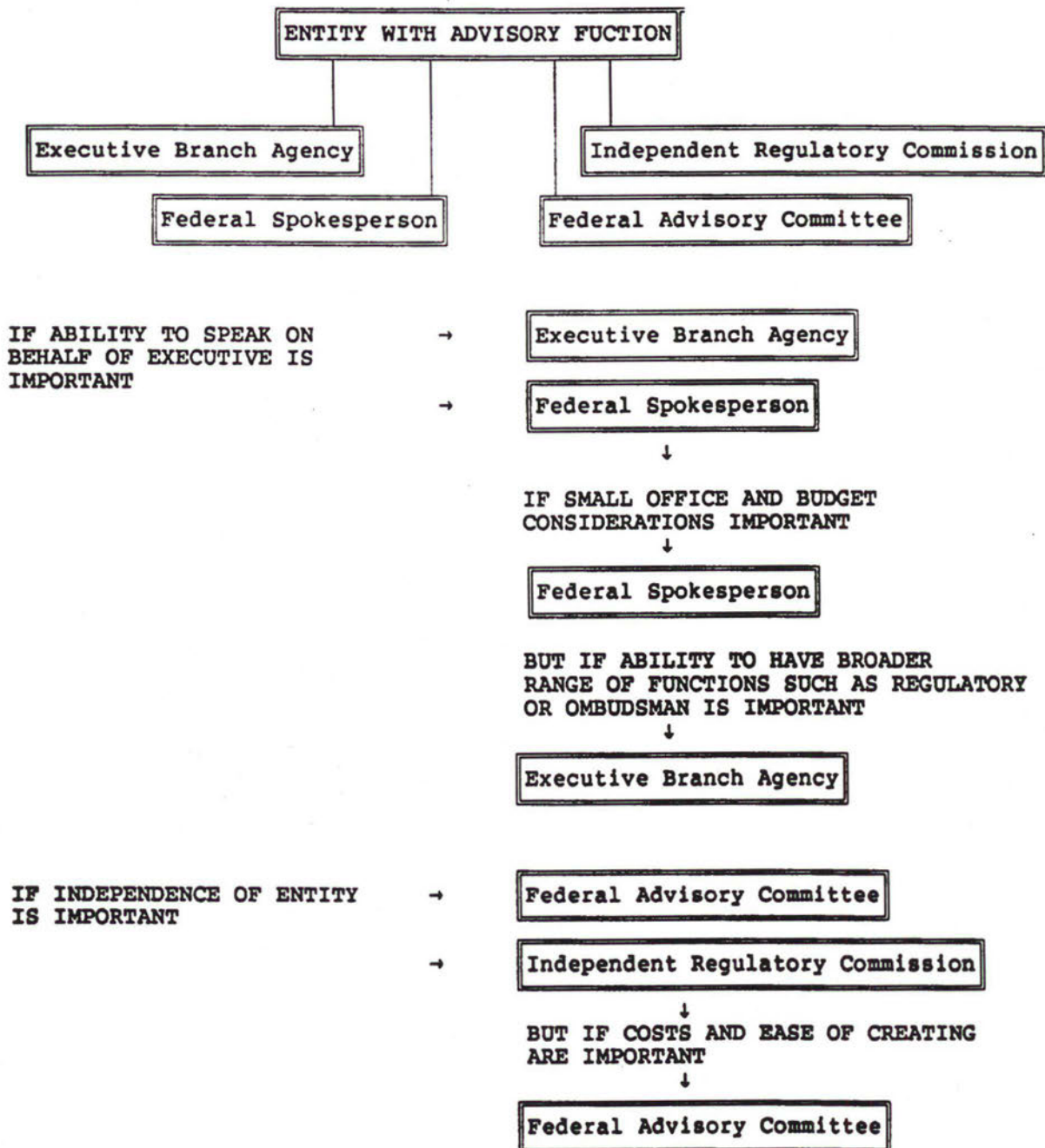
TABLE 1 - List of Placement Options with Range of *Potential* Functions that Could be Performed

PLACEMENT →				
FUNCTIONS ↓	PLACED WITHIN EXECUTIVE BRANCH EXEC BRANCH AGENCY	PLACED WITHIN EXECUTIVE BRANCH SPOKESPERSON	PLACED OUTSIDE EXECUTIVE BRANCH INDEPENDENT REGULATORY COMMISSION	PLACED AS A FEDERAL ADVISORY COMMITTEE
REGULATORY	✓		✓	
ADVISORY	✓	✓	✓	✓
EDUCATIONAL/ RESEARCH	✓	✓	✓	✓
OMBUDSMAN	✓		✓	
REPRESENTATIONAL	✓	✓		

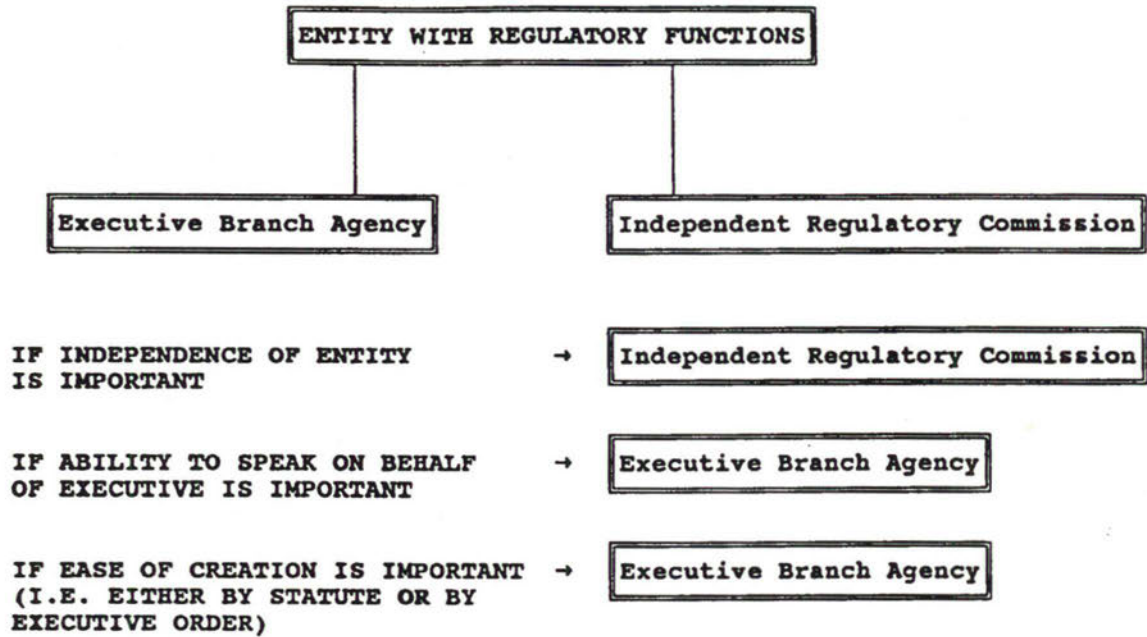
SAMPLE DECISION TREES

Although there are many possible choices that can be made based on the discussions of the various options in Section IV, several *sample* decisional trees are set forth below for illustrative purposes.

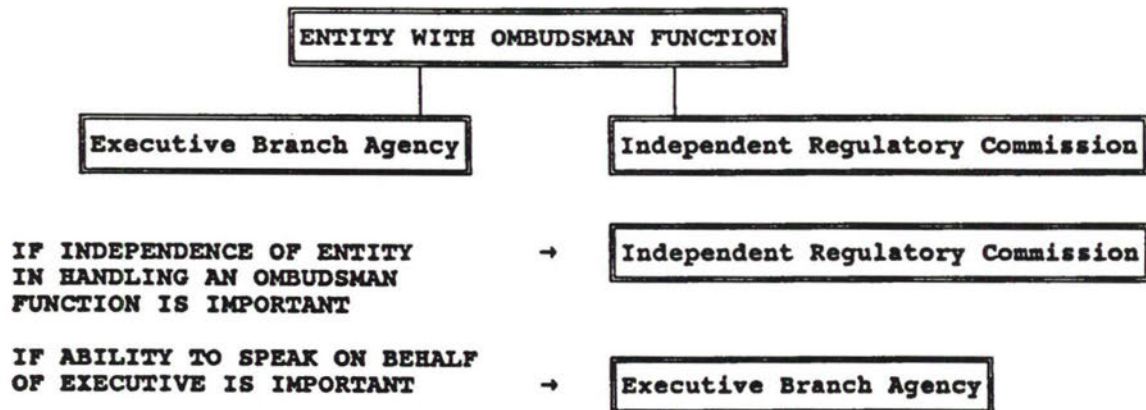
SAMPLE 1



SAMPLE 2



SAMPLE 3



**EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
Washington, D.C. 20503-0001**

LRM NO: 5426

FILE NO: 2492

8/28/96

LEGISLATIVE REFERRAL MEMORANDUMTotal Page(s): 9

TO: Legislative Liaison Officer - See Distribution below:

FROM: James JUKES *James Jukes* (for) Assistant Director for Legislative ReferenceOMB CONTACT: M. Jill GIBBONS 395-7593 Legislative Assistant's Line: 395-3454
C=US, A=TELEMAIL, P=GOV+EOP, O=OMB, OU1=LRD, S=GIBBONS, G=MARGARET, I=J
gibbons_m@a1.eop.govSUBJECT: Proposed Statement of Administration Policy RE: HR3452, Presidential and
Executive Office Accountability Act**DEADLINE: 5:00 Thursday, August 29, 1996**In accordance with OMB Circular A-19, OMB requests the views of your agency on the above subject before
advising on its relationship to the program of the President.Please advise us if this item will affect direct spending or receipts for purposes of the "Pay-As-You-Go"
provisions of Title XIII of the Omnibus Budget Reconciliation Act of 1990.COMMENTS: We understand that H.R. 3452 may go to the House floor early next week. This SAP is consistent
with the attached letter from Justice to the House Government Reform and Oversight Committee
sent on 7/24/96.

LEGISLATIVE REFERRAL MEMORANDUM
Distribution List**LRM NO: 5426****FILE NO: 2492****SUBJECT:** Proposed Statement of Administration Policy RE: HR3452, Presidential and Executive Office Accountability Act**AGENCIES:**

16-Arch. & Trans. Barriers Compliance Bd. - Kathleen Roy Johnson - 2022725434
18-Council of Economic Advisers - Liaison Officer (vacant) - 3955084
19-Council on Environmental Quality - Michelle Denton - 2023955750
29-DEFENSE - Samuel T. Brick, Jr. - 7036971305
31-Equal Employment Opportunity Comm. - Claire Gonzales - 2026634900
43-Federal Labor Relations Authority - Helenann Hirsch - 2024826500
51-General Services Administration - William R. Ratchford - 2025010563
61-JUSTICE - Andrew Fois - 2025142141
62-LABOR - Robert A. Shapiro - 2022198201
67-Merit Systems Protection Board - Steven Katz - 2026537101
71-National Council on Disability - Speed Davis - 2022722004
76-National Economic Council - Sonyia Matthews - 2024562174
83-National Security Council - Andrew D. Sens - 2024569221
88 -Office of Government Ethics - Jane Ley - 2022088022
89-Office of National Drug Control Policy - John Carnevale - 2023956736
92-Office of Personnel Management - James N. Woodruff - 2026061424
94-Occupational Safety & Health Rev Comm - William J. Gainer - 2026065380
95-Office of Science and Technology Policy - Sam Seidel - 2024566020
93-Office of the Special Counsel - Michael G. Lawrence - 2026539001
128-US Trade Representative - Fred Montgomery - 2023953475
129-VETERANS AFFAIRS - Robert Coy - 2022736666

EOP:

Bruce Overton
Frank Reeder
N. Cunningham
Elena Kagan
Kathi Whalen
Cheryl Mills
Bob Damus
Steve Aitken
Ray Kogut
Bob Rideout
Al Seferian
Bruce Long
Nancy-Ann Min
Wendy Zenker
Woody Jackson
Ed DeSeve
Peter Jacoby
Julie Haas
Nancy Schwartz
Zach Church
Bob Goldberg
Kathy Tyer
Jim Murr
Larry Matlack
John Koskinen
David Morrison
MaryJo Siclari
Kumiki Gibson
Melissa Cook
Alice Shuffield
Lisa Kountoupes
Chuck Konigsberg
Paul Weinstein

LRM NO: 5426
FILE NO: 2492

_____ Concur

_____ No Objection

_____ No Comment

_____ See proposed edits on pages _____

_____ Other: _____

_____ FAX RETURN of _____ pages, attached to this response sheet

DRAFT -- NOT FOR RELEASE

September x, 1996
(House)

H.R. 3452 - Presidential and Executive Office Accountability Act
(Mica (R) FI. and 109 cosponsors)

The Administration supports the provisions of H.R. 3452 that would apply civil rights, labor, and workplace laws to the Executive Office of the President. Most of these provisions are already being followed as a matter of law or policy by agencies within the Executive Office of the President. The Administration could support House passage of H.R. 3452, however, only if it is amended to delete the provisions establishing an Inspector General Office within the Executive Office of the President.

The Executive Office of the President is already subject to extensive scrutiny by congressional committees and the General Accounting Office. Further, the Department of Justice has advised that these provisions raise serious constitutional concerns on separation of powers grounds. These objectionable provisions would interfere significantly with the discharge of the President's constitutional authority. According to the Department of Justice, when the President is exercising exclusive constitutional authority, Congress is without authority to impose such requirements.

* * * * *



U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 24, 1996

The Honorable William F. Clinger
Chairman
Committee on Government Reform and Oversight
U.S. House of Representatives
Washington, D.C. 20015

Dear Mr. Chairman:

I am writing to express further views on H.R. 3452, the "Presidential and Executive Office Accountability Act." Previously we expressed our support for the Subcommittee's changes in the bill, which would limit the remedies to damages only.

We understand that an amendment, embodying the White House Inspector General Act of 1996, may be offered as an amendment to H.R. 3452 during the Government Reform Committee's markup of this legislation tomorrow. This amendment would interfere significantly with the discharge of the President's constitutional authority. Accordingly, the Department of Justice believes that the amendment would raise serious constitutional concerns and we strongly oppose the amendment on separation of powers grounds.

The Executive Office of the President is the designation of the President's closest advisors and aides. The amendment would add the Executive Office of the President to the list of Executive establishments subject to the Inspector General Act. An Inspector General is appointed for each covered establishment. Inspectors General, along with their staffs, are to be "independent and objective units" within their respective establishments and are "to conduct and supervise audits and investigations relating to the programs and operations of the establishment;" "to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations;" and "to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of

such programs and operations and the necessity for and progress of corrective action." 5 U.S.C. app. 3, section 2.

This general charter is supplemented with a variety of specific duties. Inspectors General are to "provide policy direction for and . . . conduct, supervise, and coordinate audits and investigations;" review legislative proposals and make recommendations for legislation relating to their respective establishments; recommend policies for and actually conduct and supervise activities to promote "economy and efficiency" in the establishment's administration; detect and prevent "fraud and abuse;" supervise and coordinate relationships between the establishment and other Federal agencies, State and local governmental agencies and non government entities to promote efficiency and prevent fraud and abuse; and keep the heads of their respective establishments and the Congress fully and currently informed about matters within their jurisdiction and recommend corrective action. Id. at section 4(a). In addition to these duties, each Inspector General is required to submit to Congress semiannual reports extensively detailing the Inspector General's activities and findings from the preceding period. Id. at section 5.

To carry out these duties, Inspectors General are vested with wide-ranging authority. Among other things, they are allowed access to all records, documents, and other materials relating to their respective establishments that pertain to their duties, and are authorized to make such investigations and reports as they deem "necessary or desirable." Id. at section 6(a).

In discharging their authority, Inspectors General are to report to and be under the general supervision of the heads of the establishments to which they are assigned. However, the head of an establishment may not prohibit or prevent the Inspector General from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena during the course of any audit or investigation. Id. at section 3(a).

The amendment would depart somewhat from the existing framework under the Inspector General Act. The Inspector General in the Executive Office of the President would be subject to the authority, direction, and control of the President with respect to audits or investigations or the issuance of subpoenas that require access to information in any of six categories.¹ The

¹ The categories are ongoing criminal investigations or proceedings, undercover operations, the identity of confidential sources, deliberations and decisions on policy matters, intelligence or counterintelligence matters, or other matters the disclosure of which constitute a serious threat to national

President would be permitted to prohibit such an audit, investigation, or subpoena, but only after the Inspector General had decided to initiate such action and only if the President determined that "the disclosure of that information would interfere with the core functions of the constitutional responsibilities of the President" and that "the prohibition is necessary to prevent the disclosure of that information." Id. at section 3. If the President exercised this preventive power, he would be required, within 30 days, to submit in writing the reasons for the determinations regarding interference with constitutional responsibilities and the possibility of disclosure to the Inspector General. The Inspector General, in turn, would be required to transmit a copy of the President's submission to specified congressional committees. In addition, the Inspector General would be required to include a description of the episode in the public semiannual report.

These provisions would raise serious concerns about intrusion on the President's constitutional responsibilities. The Constitution assigns a variety of powers exclusively to the President. Examples include the powers to nominate Federal officers, grant reprieves and pardons, act as commander in chief, and receive ambassadors and other public ministers. See U.S. Const. art. II. Congress may not intrude upon the President's exercise of these exclusive powers. See, e.g., Public Citizen v. United States Department of Justice, 401 U.S. 440 (1968) (Kennedy, J., concurring); Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam); United States v. Klein, 80 U.S. (13 Wall.) 120 (1872); Ex Parte Garland, 71 U.S. (4 Wall.) 333 (1866). Yet the amendment threatens just such an intrusion.

Even as to those exclusive powers encompassed within one of the six categories where the President may stop an audit, investigation, or subpoena, the bill would intrude upon the executive function. The Inspector General would have authority to investigate, audit, and issue subpoenas in these areas unless the President prevented the Inspector General from exercising the authority. The President could act only after the Inspector General decided to investigate, audit, or issue a subpoena, and, even then, the President would have to make written findings and submit those findings to the Inspector General who would transmit them to Congress. In these findings, the President would have to determine that "disclosure" of the information would "interfere with the core functions of the constitutional responsibilities of the President." But where the President is exercising, or has exercised, exclusive constitutional authority, Congress is wholly without authority to impose such requirements on the President or the President's advisors.

security or cause significant impairment to the national interest. See section 3 (adding section 8F(a) to 5 U.S.C. app. 3).

Furthermore, it is far from clear that all investigations, audits, or subpoenas concerning the exercise of exclusive constitutional powers would even fall within any of the six categories as to which the President would have preventive authority. For example, unless the deliberations of the President and his advisors regarding whom to nominate for a Federal office are "policy matters," the President would be without statutory authority to prohibit the Inspector General from performing investigations and audits of the exercise of that power or from reporting to Congress on these matters. Another example is the pardon power. Even if the grant of a reprieve or pardon is a "criminal . . . proceeding[]," this category applies only to "ongoing" proceedings. Thus, the bill would subject the President's deliberations on pardons that already have been granted to investigation and audit, and ultimately disclosure. The Constitution prohibits Congress from doing this.

With regard to those presidential powers that are not exclusive -- powers in those spheres where Congress possesses authority to legislate -- the doctrine of separation of powers still limits Congress's ability to adopt legislation that infringes on the President's constitutional role. In this area, a bill's validity depends on "the extent to which the bill prevents the Executive Branch from performing its constitutionally assigned functions." Nixon v. Administrator of Gen. Servs., 433 U.S. 425, 443 (1977); see Morrison v. Olson, 487 U.S. 654 (1988); CFTC v. Schor, 478 U.S. 833 (1986). "Only where the potential for disruption is present must we then determine whether that impact is justified by an overriding need to promote objectives within the constitutional authority of Congress." Administrator of Gen. Servs., 425 U.S. at 443.

Here, where the bill would invade powers exclusively committed to the President, it is unnecessary also to identify all of the ways in which the bill could invalidly intrude on the President's powers that are not exclusive. Rather, we note only that the amendment would create a strong potential for extensive interference with the ability of the President to perform all of his constitutional functions. At the least, the necessity for the President's constant vigilance about possible intrusions on his exclusive powers would impede the President's discharge of his non exclusive constitutional powers. As we have recently observed, "the Constitution's very structure suggests the importance of maintaining the 'hallmarks of executive administration essential to effective action.'" The Constitutional Separation of Powers between the President and Congress at 12 (May 7, 1996) (quoting Myers v. United States, 272 U.S. 52, 134 (1926)). Application of the Inspector General Act to the Executive Office of the President would seriously undermine this constitutional structure and this should be strongly resisted.

Thank you for the opportunity to present our views on H.R. 3452. The Office of Management and Budget advises that there is no objection to the submission of this letter from the standpoint of the Administration's program.

Sincerely,


Andrew Foia
Assistant Attorney General

cc: The Honorable Cardiss Collins
Ranking Minority Member
Committee on Government Reform and Oversight

The Honorable Steve Horn
Chair
Subcommittee on Government Management,
Information and Technology
Committee on Government Reform and Oversight

The Honorable Carolyn Maloney
Ranking Minority Member
Subcommittee on Government Management,
Information and Technology
Committee on Government Reform and Oversight

Remote Sensing Satellites and Privacy: a framework for policy assessment¹

TIMOTHY J. BRENNAN

University of Maryland Graduate School, Baltimore, MD 21228-5398, USA

MOLLY K. MACAULEY

Resources for the Future, Washington, DC 20036, USA

ABSTRACT Current and forthcoming capabilities of remote sensing technology will affect the ease with which satellites provide newer or less expensive means for uncovering otherwise private information. Consequently, RSS (Remote Sensing Satellites) technology is moving from the relatively obscure domains of oil companies and military strategists to the attention of those concerned with privacy rights and the social, political, and economic consequences of access to and distribution of information. We explicate factors determining how, if at all, to control the use and availability of information gathered by remote sensing satellites. While we discuss the intrinsic value of privacy, we emphasize the economic and social objectives privacy rights instrumentally promote, such as incentives to generate information and to promote competition or cooperation. To evaluate the need for policy regarding RSS data flows, we propose some generalizations on the effects and desirability of RSS-supplied information. An important consideration is the extent to which relations between the observer and the observed should be regarded as adversarial or complementary. Applying the framework to four categories of problematic situations, depending upon whether the observer or the observed are private parties or governmental entities, illuminates the effects RSS may have on market competition, political systems, civil liberties, and international agreements.

1. Introduction

When the Chernobyl nuclear reactor in what is now Ukraine imploded in 1986, the world learned of it via the use of satellites used to photograph the surface of the earth. These satellites, known as "remote sensing satellites", have heretofore been primarily used for fairly large scale examination or monitoring of the earth's environment and activities on the earth's surface. A typical use of remote sensing satellites has been to identify geological formations likely to contain valuable natural resources, particularly petroleum reserves. The United States and other governments have used more sophisticated satellite reconnaissance systems to observe troop movements and weapons deployment by potential adversaries.

In varying degrees of technological capability, remote sensing satellites have

been available for three decades, virtually since humans have had the ability to place spacecraft into earth orbit. Viewed more broadly, remote sensing via satellite is an extension of an ability already available through other means of aerial photography (such as aircraft). However, new developments are bringing remote sensing satellite technology from the relatively obscure domains of oil companies and military strategists to the attention of US policy makers and others concerned with the social, political, and economic consequences of access to and distribution of information.

One such development is the increasing prominence of information technology in public policy making generally and in privacy infringement in particular.² Speculation and debate over the funding, capability, pricing, and industrial organization of the "National Information Infrastructure" is but one prominent manifestation of this interest. The use of telecommunications technology for billing and electronic funds transfer, data gathering and storage, transportation and energy control, entertainment delivery, and message interception and encryption are all stimulating concern with the degree to which persons and governments should be permitted access to information about or generated by other persons and governments (Trubow, 1990; Benjamin, 1991; Bing, 1993; Lee, 1993; US Congress, Office of Technology Assessment, 1993; Onsrud *et al.*, 1994). The evaluation, design, and implementation of privacy policies in the wake of the increasing capability of electronic information technology are complicated further by the trend away from a world where a single private or public telephone company controls everything, to a realm of disaggregated, proprietary, sometimes interconnected and sometimes competing networks.

Both technological advances and economic restructuring apply to remote sensing satellites. In the not too distant future the resolution of images from satellite photographs will enable observers to identify objects no larger than a metre in size, and perhaps smaller. This will allow detailed observation of personal movements, objects stored and used on private land, corporate production runs and inventories, and public personnel and military deployments. Moreover, within the last decade the ability to generate and sell such images has become the province of international, private markets. Consequently, the technological means of supplying these observations via satellite is no longer restricted to those few governments capable of space exploration. Remote sensing satellite photography has become widely available to private parties and government entities, who can contract for images through a number of unregulated service providers competing in international markets.

While technological advances and economic reorganization are rocketing remote sensing satellites up the policy charts, concurrent developments in US constitutional law are raising the possibility that persons are becoming ever more vulnerable to unauthorized searches, particularly by law enforcement agencies.³ An important instructive example is *Florida v. Riley*.⁴ In that case, the state of Florida convicted Michael Riley of possession of marijuana, using photographs taken from a helicopter hovering four hundred feet above a greenhouse (with missing roof panels) on Mr Riley's property. Mr Riley appealed his conviction, arguing that the helicopter overflights, undertaken without warrant, violated his Fourth Amendment rights against unreasonable searches. The US Supreme Court upheld his conviction, reversing both the Florida Court of Appeals and the Florida Supreme Court. It found that Riley "could not reasonably have expected that his greenhouse was protected from

public or official observation from a helicopter", and that he had not met his burden of showing that such flights were either sufficiently rare or outside legal airspace to justify such an expectation.⁵ This decision, following similar decisions limiting constitutional protections against warrantless searches, suggests that using remote sensing satellites to gather ostensibly private information is likely to be unconstrained by law or policy absent new legislation or, at least in the US, significant reversals of recent constitutional interpretations.

Our purpose here is to explicate the considerations policy makers should analyse in determining how, if at all, to control the use and availability of information gathered by remote sensing satellites. Section 2 describes the current and forthcoming capabilities of remote sensing technology, including the ease (or lack thereof) with which satellites provide newer or less expensive means for uncovering otherwise private information. Section 3 offers a framework for evaluating the need for policy regarding RSS data flows. While we discuss the intrinsic value of privacy, we emphasize the economic and social objectives privacy rights instrumentally promote, such as incentives to generate information and to promote competition or co-operation. We propose some generalizations on the effects and desirability of RSS-supplied information, based on the relationships between the observer and the observed. Section 4 applies the framework to four categories of problematic situations, depending upon whether the observer or the observed are private parties or governmental entities. Section 5 makes some brief concluding remarks regarding policy.

2. Remote sensing satellites—capabilities and availability

Satellite remote sensing operates by way of sensors mounted on spacecraft orbiting several hundred miles above the earth's surface. The sensors measure reflected solar radiation, or in some cases, emit their own radiation and measure the amount reflected back. Recording and transmitting devices collect and send the data to earth. Parameters of the spacecraft's orbit determine how frequently the craft will pass over the same area on the earth; typically it is once every couple of days⁶.

The information content of remote sensing data depends on the spectral and spatial resolution of the sensors. Spectral resolution is the distinguishing of an object based on its own radiated energy (e.g. sand vs deciduous forest) or in contrast with the object's background (e.g. a ship on the ocean). Spatial resolution is the distinguishing of objects based on their size. Sensors operated for national security purposes are reportedly able to distinguish objects of several centimetres (Steele, 1991, p. 318), such as numbers on licence plates. At the present time, sensors operated by or marketed to civilians generate images in ranges from thirty down to five metres (Steele, 1991, p. 319).⁷

All remote sensing satellites functioning today are government-owned and operated; these include civilian satellites launched by the United States, the former USSR, Japan, Canada, France, India, and Europe. Article II of the Outer Space Treaty (United Nations, 27 Jan, 1967) grants the right of satellites to pass over international boundaries with impunity. Property rights to the data reside with the governments owning the spacecraft, although non-binding (and much debated) UN principles on remote sensing address access and distribution of data among sensing and sensed states (United Nations, 1987). States that possess information useful for averting harmful phenomena are required to disclose the

information to concerned states, for instance. More generally, information available to sensing states is to be made available to sensed states on the same terms governing availability in the sensing states.

Historically, in addition to owning and operating the RSS spacecraft, governments have also managed data distribution, access, and pricing. More recently, quasi-public institutions have been given licences by their respective governments (including the US, Russia, and France) to sell data commercially. In the cases of both public and quasi-public management of the data a variety of pricing policies govern data sales, including "free" data made available to government agencies and scientific researchers, data sold at the cost of reproduction to these entities as well as the private sector, and data sold at closer to "market" prices. Data pricing policy remains an unsettled public policy issue, however, as governments seek to balance the competing objectives of maximizing data availability by distributing the data freely, and recouping at least some operating and/or investment costs of the satellite systems by charging for the data. Charging no or low prices for data, and the absence of studies of the value of the content of the data, have rendered it quite difficult to measure the net benefits of investment in the systems. The calculus is further complicated by the public and private goods nature of the information, in that it has both public value (for example, environmental monitoring) and private value (for instance, geologic exploration).⁸

Beginning in 1993, the organization of the remote sensing industry began to change significantly. For the first time, private firms proposed what most experts see as viable business plans for the launch and operation, beginning in the late 1990s, of remote sensing satellites exclusively for commercial gain. Moreover, the sensors would operate at one- to three-metre spatial resolution—much higher resolution than previously available for non-military purposes. Very detailed data, collected remotely and concerning a host of activities, will now be commercially available and are likely to introduce new issues in the control and use of information. The types of information able to be collected are likely to be virtually unlimited, including data about use of land and other resources; industrial activities, including some kinds of air and water emissions; and other natural and anthropogenic processes.

3. Justifications for privacy rights

To understand how this availability of the capabilities of remote sensing via satellite is worthy of policy concern, we begin with some generalizations about the ethical and economic consequences of the distribution and use of the sort of private information these satellites may be able to gather. As noted earlier, we emphasize here the benefits and costs of privacy and its loss as instrumental tools for achieving social, political and economic goals. These effects will depend on the relationships among the observer, the observed, and relevant third parties. However, no discussion of privacy is complete without assessing values associated with the intrinsic worth of personhood which privacy may also protect.

3.1. *Intrinsic and instrumental foundations for privacy rights: personhood, consent, and efficiency*

Two dimensions of the various definitions of privacy figure prominently in the

literature (Schoeman, 1984). The first, typified by the aphorisms "a man's home is his castle" and "the right to be let alone" (Hixson, 1987 pp. 13, 28), is based on the capacity of the individual to assert situations in which he or she can act without actual or potential concern with the actions of others. This would include being free from unwanted calls or visits, not having to see or (over)hear neighbours, and other means by which one establishes a separate physical and mental sphere of existence for one's self. Along with this spatial dimension of privacy, there is a somewhat related but conceptually separate dimension associated with information control. Along this second dimension, one would define privacy in terms of the information by or about an agent which that agent can effectively conceal from others (Posner, 1983; Wasserstrom, 1984). As such, this informational dimension of privacy may apply to groups, corporations or governments, as well as individuals.

Privacy in its spatial and informational aspects protects both intrinsic values associated with personhood and instrumental values associated with the ability of agents to exploit information to achieve separate and collective goals. One category of intrinsic values that privacy protects relates to the *content* of the space and information protected, insofar as that space and information are themselves morally important constituents of what it means to be a person (Reiman, 1984; Griffin, 1990, pp. 228–233). A second is that space and information control are necessary for the preservation of other important constituents of personhood. These include the ability to maintain social relationships (Fried, 1984; Rachels, 1984), to generate respect for personhood (Benn, 1984), and to preserve the ability to render autonomous consent (Gavison, 1984).

As these arguments follow directly or indirectly from the intrinsic values over personhood, they do not lend a great deal of support for rights of collective organizations—churches, corporations, clubs, and governments—to control information about themselves or to delineate separate space. More notably, these intrinsic considerations are, of necessity, grounded in moral intuitions regarding intrinsic worth, the evaluation of which is beyond our scope here.⁹ Much of the controversy over privacy in general, and the use of remote sensing technology in particular, can be illuminated by looking at an instrumental approach, in which we treat privacy as one of a host of legal constructions designed to see that information is produced and distributed in such a way as to maximize social benefits at the least cost.¹⁰

This conception of privacy follows from Coase's characterization of property rights not as a manifestation of secure, intrinsically valuable relations between persons and things, but as a tool for ensuring that mutually agreeable transactions result in the allocation of things to those persons who can put them to the most valuable use (Coase, 1960).¹¹ A tenet of the so-called "Coase theorem" is that if the costs of these transactions are low and wealth effects are inconsequential, it does not matter *who* gets the property right, as long as someone does; *ex post* transactions will ensure that the resource is used efficiently. If not, courts or legislatures may need to assign rights to particular parties, to promote distributive equity or to increase the chances that the rights will be put to an efficient use (Posner, 1992, pp. 49–54).

Along these lines, privacy rights *vis-à-vis* remote sensing technology could be considered as just another kind of property right, in this case over the ability to control a delineated personal space or access to specified information. If the Coase theorem holds, privacy rights would not matter. If exclusive control over

the information is more valuable to the observed than access is to the observer, then the observed could, in principle, pay the observer not to observe. However, there are several reasons to think that RSS information may not satisfy the assumptions of the Coase theorem, and that it matters who has the right. Considerations warranting granting control rights to the observed are that there is an effectively unlimited number of potential observers who would need to be bought off, thus precluding effective control even if the value of the information to the observer exceeds the value to the observed. The flip side of the coin is that granting control to observed parties may lead to excessive restrictions on remote observation, where permission from multiple parties would be necessary before an observer could use or market an image. When there is but one observed party and one interested observer, e.g. two countries in a bilateral trade agreement, the absence of competitive opportunities and inevitable asymmetric information may prevent efficient resolution of whether RSS observation should be permitted.¹² The fact that a party in country A may employ an RSS firm in country B, leasing technology provided by country C, to observe someone in country D exacerbates any problems in reaching mutually agreeable and enforceable bargains.

In light of these complications, it would be unwise to reach a categorical judgment that RSS technology should either be unfettered or proscribed. The task for the policy maker is to identify conditions enabling qualitative predictions regarding the effects and desirability of permitting remote sensing. We begin by examining the consequences of observing private information in general, and then apply our findings to remote satellite sensing.

3.2. *Adversarial and cooperative relationships between the observer and the observed*

From the standpoint of the economics of information, invasions of privacy in general, and remote satellite sensing in particular, reduce or eliminate the possibility that the observed will know something about herself that the observer does not know. One way of viewing the situation is that the observed is less able to maintain exclusive use and control of this information; a second way is that remote sensing reduces asymmetry between the observer and the observed. The complex effects of exclusivity and asymmetry in information have been extensively investigated (Reinganum, 1989; Tirole, 1989; Hirshleifer & Riley, 1992). In contexts most likely to pertain to remote sensing, the likely effects of eliminating exclusivity and asymmetry appear to depend upon whether the relationships between the observer and the observed are adversarial or cooperative.

A useful way to present these effects is to distinguish *ex post* effects on the relationships between the observed and observed, i.e. where the agent to be observed already has the information sought by the observer, from *ex ante* effects of the prospect of *ex post* observation on the incentives to generate that information. Consider first some of the *ex post* effects in situations where the observed and observer are adversaries. If they are competitors in economic markets, the intensity of that competition will likely be reduced. For example, the value of plans to cut price, increase production runs, and change product designs can fall when a firm knows that its competitor can learn about those plans and respond more quickly with countering strategies.¹³ A similar conclusion holds if the competitors are governments engaged in diplomatic conflict. In general, we

would expect that the inability to keep information private will limit the intensity of competition based on that information.¹⁴

That inability to keep information private renders it less valuable *ex post* for adversarial purposes implies that the prospect of observation will reduce *ex ante* incentives to generate such information. Perhaps the clearest examples arise in intellectual property situations. Persons will be less likely to incur the cost in time, energy, and material in undertaking research or producing artistic works if they cannot retain sufficient control over the information embodied in the fruits of those efforts to recoup their expenses. Patent and copyright law offer some assurance of such control but, as Posner (1983, p. 243) observes, "[S]ecrecy is an important social instrument for encouraging the production of information, especially in settings where the formal rights system in intellectual property is undeveloped." In the case of RSS, such "undeveloped" settings include, in some cases, the actual undertaking of R&D expenses themselves (when these can be viewed from space—say, through changes in physical plant or plant operations), resource exploration, or commercialization plans (again, when manifested in actions viewable from space), none of which is directly protected through property law.

Different conclusions follow regarding the effects of observation when the relationship between the observer and the observed is characterized by the intent to cooperate. Such relationships typically include those between buyers and sellers, who achieve gains from the ability to trade, and between principals and agents, who can mutually benefit when the latter can successfully work to achieve the former's goals. In these contexts, eliminating information asymmetries can help make the co-operation work better. *Ex post*, the ability of an observer to watch an observed party will limit the latter's incentive to take advantage of the former. For example, if the observer is a rental car company and the observed is a renter, the ability of the former to observe will keep the latter from abusing the rented car. A more general set of examples is that parties are more likely to enter into contracts with each other—a form of cooperation—if breaches of those contracts can be prevented through penalties based on their detection (this *ex post* exploitation of an on-going relationship is known as *moral hazard*). As we discuss below, examples where RSS data may improve co-operative arrangements in this context include monitoring environmental degradation or the use of other common property resources.

Observation can improve the prospects for mutual co-operation when the information exists *ex ante*. Otherwise, cooperation can be rendered impossible through *adverse selection*. The classic example, due to Akerlof (1970), involves the market for used cars, under the assumption that buyers cannot observe what sellers know to be true about the quality of the cars sold. Inability to verify the quality of a particular car means that buyers would pay a price reflecting the average expected value of a car. Sellers who know they have better cars would tend to hold them off the market. Doing so depresses the average price, further encouraging sellers of better cars not to sell, eventually leaving only the lemons. To the extent that observation eliminates the asymmetry between the buyer and seller, both should find it easier to reach beneficial agreements.

While the discussion to this point emphasizes reductions in information asymmetries, it is crucially important to recognize that, more than many other observation technologies, remote sensing satellites may also *create other* asymmetries in information. Most important, the observed does not know that

previously private information is now in the hands of an observer. With terrestrial observation, the observed party has, at least in principle, the ability to look back at the observer along the same line of sight, and with the same observational equipment. Aerial observation provides a natural warning, through the noise that airplanes and helicopters make. In contrast, observed persons will typically have no direct way of knowing that they are the subject of high-resolution orbital photography. The satellites cannot be detected from the ground very easily, and, even if they were, parties on the ground will have no way to determine whether the satellite is photographing them, some other terrestrial feature, or nothing at all. To some extent, sophisticated parties, knowledgeable of the cost and capabilities of RSS technology, might be able to infer the likelihood that their activities are under observation. If an observed party knows that benefits of a satellite photograph of its activities to an observer exceed the commercial price of these photographs, it would be irrational not to expect that one is being observed. Still, RSS policy formulation should take into account the strong possibility that while RSS reduces advantages to the observed party from having private information, it may confer strategic benefits to the observer from the secrecy of the observation.

These considerations suggest a first generalization: improving the ability of observers to obtain information from the observed will inhibit rivalry and promote cooperation between them. Remote sensing satellites will have these effects to the extent that they inhibit exclusivity and eliminate asymmetry although, as just noted, they may create new asymmetries just as they eliminate old ones. Whether inhibiting rivalry or promoting co-operation is good or bad is the subject to which we now turn.

3.3. Substitution and complementarity between the observer and the observed

Common wisdom typically regards adversarial relationships as bad and co-operative relationships as good. If reducing exclusivity and asymmetry does generally inhibit rivalry and promote co-operation, it follows that technologies such as RSS that permit the invasion of privacy are beneficial, at least on instrumental grounds. As some of the examples supporting that generalization indicate, however, the common wisdom is not always valid. The most obvious example of the benefits of rivalry and the costs of co-operation is when the rivals are competitors in economic markets. Since Adam Smith (1953, orig. 1776), self-interested rivalry has been recognized as providing the impetus for sellers to develop and supply the goods and services buyers demand and at the lowest price consistent with recovering costs. Conversely, the premise that co-operation among competitors is generally bad underlies antitrust and competition policy laws imposing civil and criminal penalties for fixing prices, rigging bids, and allocating customers.

The common wisdom did not become that by perverse accident. In numerous contexts, co-operation rather than rivalry promotes the interests of the general public. The ability to find and purchase a good at a reasonable price inherently involves extensive co-ordination among workers, capitalists, resource suppliers, manufacturers, wholesalers, distributors, and retailers. "Firms" themselves have been regarded as essentially just collections of implicit and explicit contractual obligations designed toward common business objectives (Alchian & Demsetz, 1972). Other social institutions that provide collective goods for their members—

families, churches, associations, local and national governments—depend on co-operation to achieve those ends. In the largest context, international agreements to secure peace or preserve the environment require co-operation as well. To the extent the first generalization holds, the ability of parties in these co-operative contexts to observe each others' relevant actions should ameliorate adverse selection, discourage moral hazard, and increase the incentives and effectiveness of this co-operation.

As with the above discussion of the effects of remote sensing on informational asymmetry, there is a noteworthy qualification. In many cases, the motivation for rivalry is not to profit from the creation of new benefits, e.g. from lower prices, but from the opportunity to capture benefits that have been or would be reaped by others. Examples from the economic literature include inefficient patent races (Hirshleifer & Riley, 1992, pp. 266–271), excessive entry into non-competitive markets (Schwartz, 1989), and “rent-seeking”, i.e. expenditures to achieve government protection of one's profits from competition (Spulber, 1989, pp. 82–83). In these cases, the underlying objectives—innovation, lower prices, freedom to petition the government—are sufficiently compelling that the theoretical possibility of excessive activity has not warranted policy intervention. We see no reason to treat rivalry differently in assessing remote satellite sensing.

These observations suggest a second generalization: when the observed and observing parties provide goods and services that *substitute* for one another, i.e. when dealing with one of them reduces the need to deal with the other, then adversarial relationships are good, co-operation bad, and technological threats to exclusivity of information are undesirable. When the observed and observing parties provide goods and service that *complement* one another, i.e. where dealing with one encourages dealing with the other, then rivalry is undesirable, co-operation is good, and the ability for parties to observe each other becomes good.¹⁵ Combining this generalization with the above generalization regarding the effects of remote sensing leads to a third observation: RSS technology is likely to be beneficial when parties provide complements; less likely to be beneficial when they provide substitutes—recognizing that secret, unanticipated observation via satellite may mitigate these benefits.

4. Applications within and between the public and private sectors

These policy generalizations involve broad assessments of the justifications for private control of information and the effects of observations that prevent such control. To apply these specifically to remote sensing satellites, we identify four contexts depending upon whether the observer is a private party or a government, and whether the observed is a private party or government.

4.1. Private parties as both observed and observer

We expect that for the reasonably foreseeable future, the expense of RSS photographs will imply that the likely private purchasers of such data will be business enterprises rather than individuals. Consequently, the privacy implications created by RSS technology in the private sector are likely to involve the potential for various forms of industrial espionage. The distinction between substitutes and complements probably most clearly informs policy in this context. One important industrial use of satellite photography would be to

monitor collusive agreements among firms selling substitute products in competition with one another. Such photographs could allow firms to tell when their ostensible cartel partners were increasing production runs or delivering products into territories reserved for other sellers, in violation of price-fixing or market allocation agreements. The ability to detect "cheating" on pacts not to compete is a prerequisite for their enforcement (Carlton & Perloff, 1990, p. 223). In this case, by permitting easier enforcement of collusive arrangements, RSS may facilitate the economic harms associated with monopoly.

RSS will typically have more benign effects when the relationships between the private parties are complementary. For example, suppose an automobile manufacturer and one of its parts suppliers enter into a contract stipulating that the supplier sell exclusively to that manufacturer. Rationales for such exclusion include a guarantee that the supplier does not disclose the automobile manufacturer's proprietary information to other car companies, and that the parts supplier exercises appropriate quality control efforts on the manufacturer's behalf (Brennan, 1989b). RSS technology might help prevent breach of this contract, by permitting the automobile manufacturer to observe whether the supplier is shipping parts to other car makers. A perhaps less benign example of the ability of RSS to ensure exclusive dealing might be allowing firms to monitor employees' outside activities, e.g. by checking to see that they were not out for a leisurely drive to the beach on a day when they called in sick. Still, even in this case one would expect that workers would be compensated, both for the potential loss in privacy and because the technology would allow employers to deter shirking, making workers more valuable and raising their wages and salaries.

4.2. *Government as observed; person as observer*

Since the government and its citizens are agents of a different kind, one would expect that their relationship would be characterized by complementarity rather than substitutability. Accordingly, we would expect that RSS technology that permits citizen observation of government activities to be beneficial. As with the private-private context, we would not expect individuals to do much direct observation of their governments. Not only is the cost of such observation likely to be great relative to the income of most persons, but the benefits of such monitoring are likely to be spread over the public at large, too thinly to be worth the observation cost to any single individual.

An exception may be observations made by private firms of commercial activity in states where industrial sectors are nationalized. The UN Principles referenced earlier that encourage observing states to share information with observed states do not address the situation of whether a private company must inform a state that it has been observed (Gabrynowicz, 1995). However, there is a private collective institution that is particularly likely to find it affordable and worthwhile to use RSS technology to observe the government—a competitive press, responding to the demands of citizens engaged in public affairs. Thus, RSS technology could promote the political values supported by freedom of the press, by combatting the consequences of asymmetric information between citizens and their state. Some of the benefits such freedoms support is akin to those associated with ensuring exclusive dealing in the above discussion. The primary gain is that press observation enables public officials to commit *credibly*

to the public that they will work on the its behalf (Brennan, 1995). Withholding information from the public may be necessary to allow the government and its officials to aggrandize themselves at the public's expense; freedom of the press to observe the government can prevent that exploitation. For example, the press might use RSS-supplied photographs to verify that public works budgets are being used on the intended land reclamation projects, and not on limousines, swimming pools, and other "perks" for the government workers.¹⁶

4.3. *Person as observed; government as observer*

The presumption that persons and governments operate at different levels, hence are inherently complementary agents in search of co-operation rather than competitive agents who should be adversarial, would imply that when the person is the observed rather than the observer and *vice versa*, elimination of informational asymmetry through RSS technology is a good thing. This is not a wholly unjustifiable position. Private compliance with government mandate, akin to government compliance with private mandate, should be in the social interest if the laws and regulations themselves procedurally and substantively reflect the consent of the governed. The obvious context for this is the enforcement of laws and regulations. RSS photography can enable the state to enforce pollution emission controls and detect other forms of criminal conduct. Evidence garnered by such technology can lead to more efficient resolution of disputes (Marks, 1989).¹⁷

However, legal and political traditions in the US regard government observation of individuals as something to be restricted unless warranted, literally, by a court as necessary to secure an important government purpose. Some of this concern reflects the intrinsic rather than instrumental justifications discussed above, with the important addition that government information may tilt the scales of justice in civil criminal proceedings inappropriately against potential defendants. Instrumental considerations may hold sway here as well. When government can observe private citizens via satellite, the latter may not be able to detect such observation. As noted above, this creates an asymmetry, mitigating the ability of RSS satellites to encourage cooperation.¹⁸ A second asymmetry, that the government can observe the individual but not *vice versa*, absent indirectly through the press, may be more important in hampering the individual's ability to compete against the state over the ability to control his or her private sphere, and to ensure that the government acts on behalf of the public rather than its self-delineated interests. To the extent that state power and individual will are substitute determinants of personal behaviour rather than complementary providers of a liberal civil environment, our generalizations suggest that RSS's propensity to hamper competition between the state and the individual may be detrimental.

The prevailing legal standard for whether government entities can observe individuals without either their consent or a judicial warrant is whether the search ran counter to the individual's "reasonable expectation of privacy".¹⁹ Steele (1991) offers numerous reasons as to why RSS observation may violate this reasonable expectation, primarily the public's lack of access to space and this expensive and unorthodox technology, and its inability to detect whether a satellite is observing them. Neither argument may prove legally compelling as

entry and competition in RSS makes it more commercially available, routine, and inexpensive.

A more significant problem is the conceptual ambiguity of a "reasonable expectation of privacy" standard. In such a phrase, "reasonable" may have a descriptive or normative meaning, and it matters considerably which meaning is at stake. Under a normative interpretation, "reasonable" would mean something like "in accord with appropriate values". Such a definition would allow a court to disallow RSS evidence gathered by a government, despite the availability of RSS technology, if collecting that evidence violated these appropriate privacy values, whatever they might be. However, the relevance of considerations such as the availability of the technology to the public and the frequency of surveillance suggests that current law relies on a descriptive interpretation, based on whether rationally a person would predict vulnerability to such observation. If a normative approach is flawed because it forces courts into making explicit philosophical judgments, the descriptive approach is flawed because it offers no assurance that any amount of privacy would be protected. Night-time KGB searches in the former Soviet Union would meet the descriptive interpretation, since no "reasonable" resident of the Soviet Union could expect not to be subject to such searches. Consequently, as long as the "reasonable expectation of privacy" standard prevails, it may only be a matter of time before a government can use RSS data to investigate and prosecute its citizens.²⁰

4.4. States as both observed and observer

The principle that RSS-generated information will deter competition and promote co-operation applies in the first instance to international relations as well as to private and private-state relationships. Nations are most prominently providers of substitutes rather than complements when they operate or oversee exports, e.g. oil or coffee. RSS technology can make it easier for countries in an export cartel to detect production or shipments beyond quotas imposed to restrict aggregate supplies, in order to maintain higher prices and generate monopoly profits. RSS may also provide a means of collecting information about the production technologies of industries in rival states or their supplies of natural resources. In these cases, as our generalizations suggest, the use of RSS technology to facilitate co-operation among parties that provide substitute goods and services is likely to be socially detrimental. In other cases, however, we would expect the activities of different nations to be complementary, in that the efforts reinforce rather than replace one another in achieving social goals. An example is the use of RSS to enforce military treaties. With the growth of concern with the environment, the use of RSS technology to monitor natural resource use and transboundary air and water pollution may be increasingly important (Macauley, 1992, p. 32).

In both of these situations RSS technology can promote international cooperation by making it easier to observe deviations from military treaties and environmental agreements. High resolution satellite photography can allow signatory nations to verify reductions in weapons or environmental emissions. However, the value in ensuring this cooperation may conflict with values associated with national sovereignty (Macauley, 1992, pp. 37-39). In addition, asymmetry in access to the technology or RSS information could put lower-income or non-spacefaring observed countries at a disadvantage, although in-

creases in the commercial availability of satellite imagery may reduce advantages more technologically advanced nations have via exclusive control of RSS. A related concern is that the use of RSS technology to reveal internal practices might result in a loss of prestige leading the observed country to withdraw from otherwise desirable international agreements. For example, disclosure of dirty industrial processes might lead a country to lose face in negotiations for environmental protection (Macauley, 1992, pp. 33, 36).

Evaluating the trade-off between the gains from international co-operation and the risks to national sovereignty will depend on one's philosophical judgment regarding the merits and content of rights associated with national self-determination (Graff, 1994)—some of which may resemble the intrinsic value arguments supporting privacy rights—against the obligation to contribute to collectively beneficial goods (Rawls, 1971, p. 111–112). Nations who wish to “cheat” on international agreements may assert such rights, potentially eliminating the civil and environmental benefits such agreements may generate. Regardless of its philosophical merits, however, national sovereignty will demand our attention as a matter of practical politics.

5. Policy lessons

Remote sensing satellite technology clearly reduces the ability of persons and governments to maintain privacy, in the sense of exercising exclusive control over information regarding their activities. The potential effects on economic markets, political systems, civil liberties, and international relations are numerous. All of these reasons, along with advancing technology, will stimulate ever increasing policy attention toward RSS.

The framework we have outlined offers some insights for the public and its officials in developing RSS policy. The plethora of possible effects of RSS technology can be classified by recognizing that using RSS to reduce informational asymmetry and exclusivity is likely to inhibit rivalry and promote cooperation. Such effects are more likely to be beneficial when the activities of observed and observing parties are complementary rather than fungible. Consequently, RSS technology should be neither banned nor unfettered. The relationships between the observed and observer will be crucial, and in many cases determinative, in ascertaining whether RSS technology should be encouraged (e.g. enforcing arms control treaties) or discouraged (facilitating cartels).

The analysis will never be perfectly simple. In some cases, RSS technology may establish new informational asymmetries, as parties will be less able to detect observation. National sovereignty may fall victim to the ability and availability of RSS. Other rights of privacy, particularly those associated with civil liberty protections against unreasonable searches, may be at risk, particularly under prevailing legal standards in the USA. However, we believe that examining remote sensing using general effects on information distribution and the identification of the kinds of situations in which such effects are more or less likely to be beneficial is a useful first step in the philosophical and policy analysis of this evolving technology.

Notes

1. This paper was written while Professor Brennan was a Gilbert White Fellow at Resources for the

Future. We gratefully acknowledge RFF's support, and note that the opinions we express here are our own and not necessarily those of RFF or anyone associated with it.

2. National security concerns arise as well; we recognize these concerns and touch upon them in section IV, but fuller treatment is outside the scope of this paper. Further discussion is contained in US Congress, Office of Technology Assessment (1987) and Davis (1992).
3. Useful reviews of recent US developments in the effects of aerial surveillance on constitutional protections against warrantless searches include Gutterman (1988), Hansen (1990), Stewart (1990), Steele (1991), and Galloway (1992). US Congress, Office of Technology Assessment (1987) discusses satellite newsgathering in the context of the first amendment.
4. 488 US 445 (1988). Other important recent US cases supporting rights of aerial searches are *California v. Ciraolo*, 476 US p. 207 (1985) (affirming the right of police to observe visually a marijuana patch from a private plane within airspace available to the public); *Dow Chemical Co. v. US*, 476 US 227 (1985) (allowing the US Environmental Protection Agency to employ commercial aerial photography to observe Dow's chemical plant, despite Dow's efforts to ensure the plant's privacy).
5. 488 US, pp. 450–451. The Supreme Court's analysis was actually a bit more complicated. Riley's conviction was upheld by a four-judge plurality opinion, with Justice O'Connor issuing a concurring opinion. Justice O'Connor differed from the plurality in arguing that the crucial factor should be the frequency of flights, rather than giving much weight to the legality of such flights under US aeronautical law, as the plurality did. Hansen (1990) p. 427; 488 US, p. 453.
6. We focus on RSS satellites operating at fairly high spatial resolution. Lower spatial resolution RSS typically involves the collection of weather data only, not other earth processes or land information.
7. Drury (1990) offers an excellent technical survey of satellite remote sensing.
8. Macauley and Toman (1991) discuss this pricing issue in depth.
9. Deontological claims for privacy rights grounded in intrinsic values, like arguments for other rights, tend to be categorical, since they by definition cannot be judged as to whether they maximize some measure of the good. The leading contemporary method for avoiding categorical didacticism is to derive these rights as the outcome of a philosophically pure bargain (Rawls, 1971). A second possible tactic follows from the implied ability of categorical rights to override considerations of social utility (Dworkin, 1977). This implies that rights holders themselves ought not be able to alienate those rights, allowing us to test rights claims against our intuitions regarding inalienability (Brennan, 1988, 1989a, 1994).
10. In other words, our discussion will emphasize "welfarist" justifications for privacy, as differentiated from aforementioned justifications to autonomy, following Sen & Williams (1983).
11. Brennan (1993) distinguishes Coase's view of property from traditional philosophical views that attempt to derive property rights from intrinsic values of ownership rather than their ability to facilitate efficient transactions. For a normative, consent-based defence of the Coasian standpoint, see Posner (1980); for criticisms, see Coleman (1980) and Dworkin (1980).
12. See Fudenberg & Tirole (1992, pp. 275–279) for a formal analysis of how asymmetric information impedes efficient resolution of bilateral negotiations.
13. We assume here that the observed and observing firms perceive the information to be accurate—that is, the expected value of the information is assumed equal to its information content, and that content is expected to be accurate.
14. It may lead to increased activity to conceal the information further, however, but we do not consider this effect here.
15. Bulow *et al.* (1985) use these terms in classifying strategic interactions.
16. As with all generalities, there are exceptions. Under some very specific and complex conditions, the public may elect to remain ignorant of its military's actions, if such ignorance will leave the military more able to deter potential aggressors with excessive force that the citizens themselves would not credibly support (Brennan, 1992). Davis (1992) suggests that RSS technology will make it "futile" for governments to keep visual information on military deployments out of the public's view, implying that this strategic rationale for secrecy may lack credibility. US Congress, Office of Technology Assessment (1987) focuses on the potential relationship among a press corps' "mediasat" satellite, national security, and the first amendment to the Constitution.
17. Gabrynowicz (1995) notes that the European Community has established a policy of using aerial and satellite remote sensing to police fraud associated with the use of agricultural subsidies.
18. Onsrud *et al.* (1994) also express concern that the observed may not have the opportunity to challenge the accuracy of the government's data or the interpretations the government makes of it.

19. *Katz. v. United States*, 389 US 347, 360 (1967) (J. Harlan, concurring). In this case, the Supreme Court found that gathering evidence through use of a listening device attached to the outside of a telephone booth was an unreasonable search and seizure, since doing so "violated the privacy upon which [Katz] justifiably relied." *Idem* p. 353.
20. In fact, this concern has arisen with the use of roadside remote sensing devices to monitor auto tail-pipe emissions; the system also includes cameras that photograph licence plate numbers.

References

- Alchian, A. & Demsetz, H. (1972) Production, information costs, and economic organization, *American Economic Review*, 62; pp. 777-795.
- Akerlof, G.A. (1970) The market for "lemons": qualitative uncertainty and the market mechanism, *Quarterly Journal of Economics*, 84, pp. 488-500.
- Benjamin, L. (1991) Privacy, computers, and personal information: toward equality and equity in an information age, *Communications and the Law*, 13; pp. 3-16.
- Benn, S.I. (1984) Privacy, freedom, and respect for persons, in: F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: an anthology*, pp. 223-224 (Cambridge, Cambridge University Press).
- Bing, J. (1993) Privacy and surveillance systems: balancing competing interests, *The International Computer Lawyer*, 10; pp. 17-23.
- Brennan, T.J. (1988) Rights, market failure, and rent control: a comment on Radin, *Philosophy and Public Affairs*, 17; pp. 66-79.
- Brennan, T.J. (1989a) The "fairness doctrine" as public policy, *Journal of Broadcasting and Electronic Media*, 33; pp. 419-440.
- Brennan, T.J. (1989b) Exclusive dealing, limiting outside activity, and conflict of interest, *Southern Economic Journal*, 56; pp. 323-335.
- Brennan, T.J. (1992) Rational ignorance: the strategic economics of military censorship, *Southern Economic Journal*, 58; pp. 966-974.
- Brennan, T.J. (1993) Copyright, property, and the right to deny, *Chicago-Kent Law Review*, 68; pp. 675-714.
- Brennan, T.J. (1994) Markets, information, and benevolence, *Economics and Philosophy*, 10; pp. 151-168.
- Brennan, T.J. (1995) Game theory and the first amendment: strategic implications of freedom of the press, in: G. Brock (Ed.) *Toward a Competitive Telecommunication Industry: selected papers from the 1994 Telecommunications Policy Research Conference*, pp. 309-301 (New York, Erlbaum).
- Bulow, J.I., Geanakoplos, J.D. & Klemperer, P.D. (1985) Multimarket oligopoly: strategic substitutes and complements, *Journal of Political Economy*, 93; pp. 488-511.
- Carlton, D.W. & Perloff, J.M. (1990) *Modern Industrial Organization* (LaPorte, IN, Harper-Collins).
- Coase, R.H. (1960) The problem of social cost, *Journal of Law and Economics*, 3; pp. 1-44.
- Coleman, J.L. (1980) Efficiency, utility, and wealth maximization, *Hofstra Law Review*, 8; pp. 509-551.
- Davis, R. (1992) Spying on the government: the media, remote sensing satellites and US national security policy, *Political Communication*, 9; pp. 191-206.
- Drury, S.A. (1990) *A Guide to Remote Sensing: interpreting images of the earth* (Oxford, Oxford University Press).
- Dworkin, R. (1977) Taking rights seriously, in: R. Dworkin (Ed.) *Taking Rights Seriously* (Cambridge, MA, Harvard University Press).
- Dworkin, R. (1980) Why efficiency? *Hofstra Law Review*, 8; pp. 563-590.
- Fried, C. (1984) Privacy: a moral analysis, in: F. D. Schoeman (Ed.) *Philosophical Dimensions of Privacy: an anthology*, pp. 203-222 (Cambridge, Cambridge University Press).
- Fudenberg, D. & Tirole, J. (1992) *Game Theory* (Cambridge, MA, MIT Press).
- Gabrynowicz, J. (1995) Inconsistent legal landscape, *Space News*, 6; 15 January, pp. 9-15.
- Galloway, R.W., Jr. (1992) Basic fourth amendment analysis, *Santa Clara Law Review*, 32; pp. 737-782.
- Gavison, R. (1984) Privacy and the limits of law, in: F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: an anthology*, pp. 346-402 (Cambridge, Cambridge University Press).
- Graff, J.A. (1994) Human rights, peoples, and the right to self-determination, in J. Baker (Ed.), *Group Rights*, pp. 186-214 (Toronto, University of Toronto Press).
- Griffin, J. (1990) *Well-Being: its meaning, measurement, and moral importance* (Oxford, Oxford University Press).
- Guterman, M. (1988) A formulation of the value and means models of the fourth amendment in the age of technologically enhanced surveillance, *Syracuse Law Review*, 39; pp. 647-735.

- Hansen, D.R. (1990) Warrantless aerial surveillance and *Florida v. Riley*: the loss of liberty, *Utah Law Review*, 1990, pp. 407-438.
- Hirshleifer, J. & Riley, J.G. (1992) *The Analytics of Uncertainty and Information* (Cambridge, Cambridge University Press).
- Hixson, R.F. (1987) *Privacy in a Public Society: human rights in conflict* (Oxford, Oxford University Press).
- Lee, L.T. (1993) U.S. telecommunications privacy policy and caller ID, *California Western Law Review*, 30; pp. 1-60.
- Macauley, M.K. (1992) Collective goods and national sovereignty: conflicting values in global information acquisition, *Proceedings of the Conference on Space Monitoring of Global Change*, pp. 31-47 (San Diego, University of California Institute on Global Conflict and Cooperation).
- Macauley, M.K. & Toman, M.A. (1991) Providing earth observation data from space: economics and institutions, *American Economic Review*, 81; pp. 38-41.
- Marks, B.S. (1989) Dispute resolution in the space age: forensic applications of earth observation satellite data through adaptation of technical standards similar to DNA fingerprinting protocols, *Ohio State Journal on Dispute Resolution*, 5; pp. 19-73.
- Onsrud, H.J., Johnson, J.P. & Lopez, X. (1994) Protecting personal privacy in using geographic information systems, *Photogrammetric Engineering and Remote Sensing*, 60; pp. 1083-1095.
- Posner, R.A. (1980) The ethical and political basis of the efficiency norm in common law adjudication, *Hofstra Law Review*, 8; pp. 487-507.
- Posner, R.A. (1983) Privacy as secrecy, in: R. Posner (Ed.) *The Economics of Justice*, pp. 231-267 (Cambridge, MA, Harvard University Press).
- Posner, R.A. (1992) *Economic Analysis of Law* (Boston, Little, Brown).
- Rachels, J. (1984) Why privacy is important, in: F. D. Schoeman (Ed.) *Philosophical Dimensions of Privacy: an anthology*, pp. 290-299 (Cambridge, Cambridge University Press).
- Rawls, J. (1971) *A Theory of Justice* (Cambridge, MA, Harvard University Press).
- Reiman, J.H. (1984) Privacy, intimacy, and personhood, in: F. D. Schoeman (Ed.) *Philosophical Dimensions of Privacy: an anthology*, pp. 300-316 (Cambridge, Cambridge University Press).
- Reinganum, J.F. (1989) the timing of innovation: research, development, and diffusion, in R. Schmalensee & R. Willig (Eds), *The Handbook of Industrial Organization*, pp. 850-908 (New York, North-Holland).
- Schoeman, F.D. (Ed.) (1984) *Philosophical Dimensions of Privacy: an anthology* (Cambridge, Cambridge University Press).
- Schwartz, M. (1989) Investments in oligopoly: welfare effects and tests for predation, *Oxford Economic Papers* (supp.) 38, pp. 37-57.
- Sen, A.K. & Williams, B. (1983) Introduction, in: A. K. Sen & B. Williams (Eds) *Utilitarianism and Beyond*, pp. 1-21 (Cambridge, Cambridge University Press).
- Smith, A. (1953, orig. 1776) *An Inquiry into the Nature and Causes of the Wealth of Nations* (Chicago, Henry Regnery).
- Spulber, D.F. (1989) *Regulation and Markets* (Cambridge, MA, MIT Press).
- Steele, L. (1991) The view from on high: satellite remote sensing technology and the fourth amendment, *High Technology Law Journal*, 6, pp. 317-334.
- Stewart, D.J. (1990) *Florida v. Riley*: the emerging standard for aerial surveillance of the curtilage, *Vanderbilt Law Review*, 43, pp. 275-295.
- Tirole, J. (1989) *The Theory of Industrial Organization* (Cambridge, MA, MIT Press).
- Trubow, G.B. (1990) Protecting information privacy in the information society, *Northern Illinois University Law Review*, 10, pp. 521-542.
- United Nations (27 Jan. 1967) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.
- United Nations (1987) Declaration of Principles Regarding the Remote Sensing of Earth from Space. 2 UN Doc. A/RES/41/65.
- United States Congress, Office of Technology Assessment (1987) *Commercial Newsgathering from Space*, OTA-TM-ISC-40 (Washington, DC, US Government Printing Office).
- United States Congress, Office of Technology Assessment (1993) *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC, US Government Printing Office).
- Wasserstrom, R.D. (1984) Privacy: some arguments and assumptions, in: F. D. Schoeman (Ed.) *Philosophical Dimensions of Privacy: an anthology*, pp. 317-332 (Cambridge, Cambridge University Press).

EXECUTIVE OFFICE OF THE PRESIDENT



THE OLD EXECUTIVE OFFICE BUILDING

COUNCIL OF ECONOMIC ADVISERS
17TH AND PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20502

Sally Katz, OMB
Joe
Michele
Chrono file
me
- Thanks

TO: Gerald Carter, Census
FAX NUMBER: 301-457-2515

OFFICE: 2430

TEL NUMBER: 301-457-2654

FROM: TIM BRENNAN

FAX NUMBER: (202) 395-6809

TEL NUMBER: (202) 395-5614

ROOM: 322

NO. OF PAGES (inc cover) 9 DATE: 9/3/96

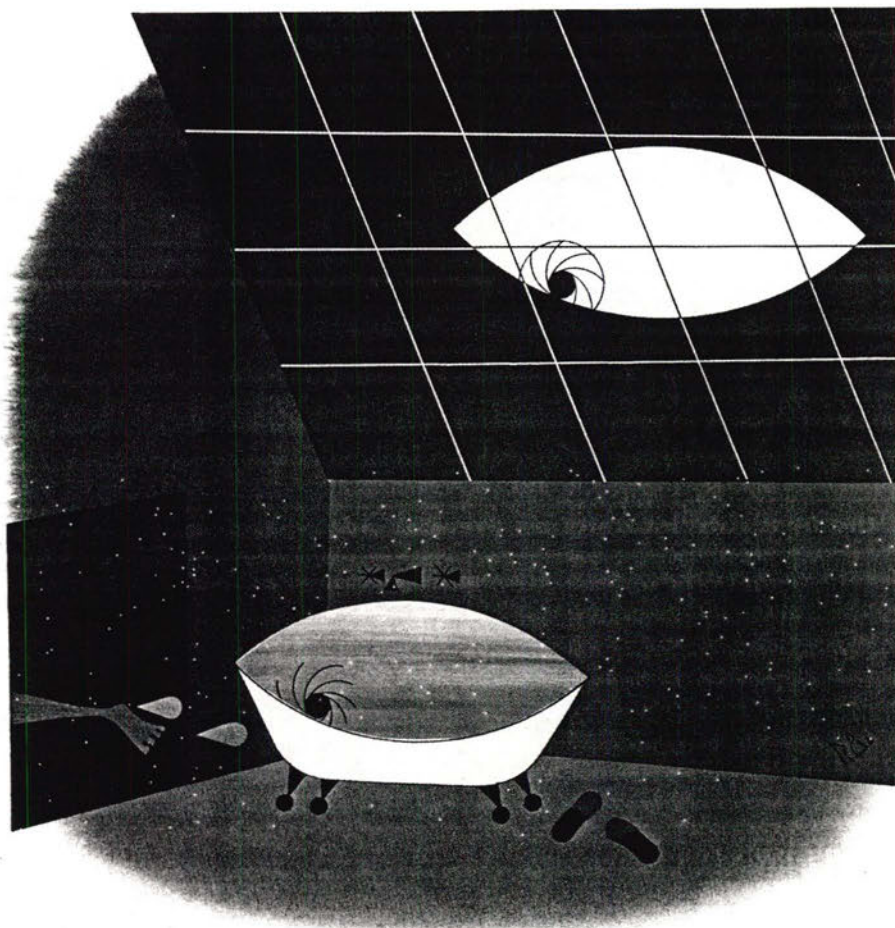
SUBJECT: 11TF Privacy Draft

MESSAGE:

Gerald,

I'm the new CEA "regulation/telecom" person, and
I was given your excellent draft privacy report to review.
I hope these (unreviewed) comments are of some use
to you.

Tim Brennan, CEA



High Resolution, Unresolved

Private companies will soon launch satellites powerful enough to spot environmental hazards—or a car in your driveway. Should we worry about snooping from space?

FOR more than thirty years spy satellites launched by the United States have been gathering a “virtual time-machine record of the earth,” as Vice President Al Gore has described it. The public has paid close to \$100 billion for that record. But national-security and personal-privacy concerns

by Mary Graham

have blocked the use of the world’s most powerful sensors to make current information about natural resources, environmental hazards, and private property in the United States available to environmental scientists, government agencies, and businesses. Because the Central Intelligence Agency is barred by

federal law from spying on Americans, it shares current environmental information about the United States only in rare instances—for example, in response to natural disasters.

Now, though, spy-satellite technology that has been used for a single purpose—espionage—with extraordinary government controls can suddenly be used for any purpose with few controls. In 1994, concerned about the post-Cold War health of the U.S. aerospace industry and fearful that foreign competition might challenge U.S. leadership in satellite technology, the Clinton Administration decided that private companies could launch satellites with high-resolution sensors previously available only to the intelligence community, and could provide information to anyone willing to pay for it. As government officials take cautious steps to share information gathered by military satellites, four U.S. companies are racing to launch satellites of their own equipped with similar technology. The first launch is scheduled for later this summer.

At a recent conference in Washington, D.C., Mark Brender, ABC’s Pentagon producer, predicted that precise pictures from space will revolutionize television news, both by freeing reporters from relying on government-provided information during international crises and by freeing viewers from relying solely on what reporters tell them. David Bohrmann, an executive producer at NBC, demonstrated how networks could use satellite pictures to simulate flyovers of troop encampments in Bosnia. At his command a technician in New York using prerecorded images zoomed in on villages, scanned rivers, and hovered over military bases, producing a moving picture that resembled a helicopter ride around the countryside.

WHAT is really at stake is the ground rules for the next phase of mapping the earth. By next year three of the four companies plan to produce images of one-meter resolution—100 times as precise as those of current civilian satellites. The ability to see hazy outlines of large buildings will be replaced with the ability to see the clear shapes of small

cars. The ability to observe the same farm or city block every sixteen days will be replaced with the ability to observe the same point every two or three days; three to six images a day of most places in the United States are promised within four years.

Fundamental issues are being decided now. When should the government be allowed to censor images to protect national security? Should fears of military snooping from space be replaced with fears of snooping by corporations or domestic agencies? Will access to satellites' most detailed pictures pass from a small cadre of military clients with top-secret clearance to a small cadre of corporate clients with the means to pay for them?

Since commercial use of this technology is new, no one has a ready framework for resolving questions about national security, the protection of privacy, and public access to information. Time-tested principles that allow the government to block information in emergencies, keep homes and their surroundings free from intrusion, and treat geographic information as a national resource can provide guidance—if they are heeded. The breadth of the government's power to censor images may be decided this fall, when the Commerce Department is expected to issue final policies setting the conditions for commercial licenses to operate satellites. Privacy questions may be decided in an international context: strict privacy rules adopted by the European Union last July require consent for the use of information that identifies an individual. They may keep companies in the United States from selling images abroad unless similar rules are approved in this country. Access questions—whether images can be copied and distributed to the public, for example—will probably be negotiated between satellite companies and their customers, including government agencies.

NO longer simply the source of spectacular views of the earth, satellite images have a new capacity to influence what people do and how they think. Using sophisticated software and powerful, inexpensive computers, businesses, government agencies, citizens' groups, and individuals can now produce layered

maps (called Geographic Information Systems, or GIS) that combine new environmental findings with information already available to the public, such as property ownership and census data. New satellites will make such maps more useful by providing high-resolution images with digital precision and offering predictable repeat visits. Neither aerial photography nor current civilian satellites like Landsat or the French SPOT can produce this combination.

The investigative powers of satellites derive not just from photography but from sensors measuring visible and invisible wavelengths of the sun's energy. These can reveal more about an object's character than can be discovered standing next to it: each species of plant, type of soil, and kind of rock or building material, for example, uniquely reflects and absorbs wavelengths. Experts add a few caveats: measures of reliability are critical; interpretation is complicated; and much of this science is still in its infancy. And like all maps, these reflect the quality of underlying information.

Information from sensors can give early warning of environmental hazards. Kass Green, the president of Pacific Meridian Resources, a mapping firm, expects that new images will help minimize the damage done by wildfires like those that sweep through urban areas such as Los Angeles and Oakland, California. For the first time, she says, it will be possible to easily distinguish asphalt, wood-shake, and synthetic-shake roofs and to assess from week to week the dryness of vegetation around homes. Planning firebreaks and other preventive measures depends on accurately predicting a fire's path.

Satellite maps can help to settle political controversies—or create them. When, for example, environmental groups and the Bush Administration clashed over how much old-growth forest in the Pacific Northwest should be protected as habitat for the spotted owl, competing layered maps produced by the Wilderness Society and the federal Forest Service provided a basis for negotiation, by clarifying different ways of defining old growth. New maps of Latin America that were completed last fall by the World Wildlife Fund have led to a debate about how to use limited conservation funds: the maps make

clear that tropical dry forests and grasslands are as important to biodiversity as rain forests, and are more severely threatened.

Satellite images can make things harder to hide. The Environmental Protection Agency has used such images to help identify hazardous-waste sites and sources of water pollution. European farmers, who receive crop subsidies of \$50 billion a year, have new reasons to submit accurate information: their planting patterns are monitored from space by the European Commission. When farm boundaries are layered over images of the countryside, infrared color codes reveal whether a field is growing barley, wheat, corn, or something else.

OF course, newly explicit images can also be used to make mischief. Foreign intelligence agencies are expected to be among the largest buyers of high-resolution images. "International security issues are serious," says Ray Williamson, a senior research scientist at the George Washington University Space Policy Institute. "Iraq would be interested in information about Saudi Arabia. Iran would like to see data about Israel. India and Pakistan would like to have information about each other. If you were concerned about troop buildup on your border, you could put in a standing order for the satellite to take a picture every time it passed over." During international conflicts this greater access could lessen the information advantage the United States has over other countries.

Some experts argue that expanded access could be beneficial. Neighboring countries might be less quick to threaten each other when troop movements were visible to all. When U.S. troops are involved in international conflicts, though, the U.S. government has a strong interest in controlling the flow of information. "One reason we were able to best the Iraqis," Williamson says, "was that we had very good information about them and they didn't know what we were doing."

To minimize security risks, the U.S. government is working to keep "shutter control"—broad latitude to turn off sensors when images might compromise "national security, international obligations and/or foreign policies." Representatives of television networks and other

news media argue that the government's authority to stop the use of satellite images should be no broader than its authority to stop the publication or airing of other sensitive information, and that exercising it should require the same judicial process.

Whatever the outcome of that debate, growing international competition means that customers who want high-resolution images will probably be able to buy them. The CIA has been cautious about declassifying spy-satellite pictures: so far only archives from 1960 to 1972 have been released to the public, and the results of a joint U.S.-Russian effort to study environmentally important sites around the world using spy satellites will be kept secret for the foreseeable future. But Russia is already selling some current two-meter images from military satellites, and France, Israel, and Japan plan to market high-resolution imagery.

WHERE to draw the line between personal privacy and the public and commercial need for information will become urgent when high-resolution surveillance is routine. For the first time, detailed pictures of every piece of private property in the United States will be routinely compiled and marketed. Commercial satellites cannot yet produce images of people, but they can show vehicles parked in driveways and structural changes to homes. They can provide images within a few hours and exact comparisons of the same property at precise intervals without giving clues about their presence—things that aerial photography cannot do.

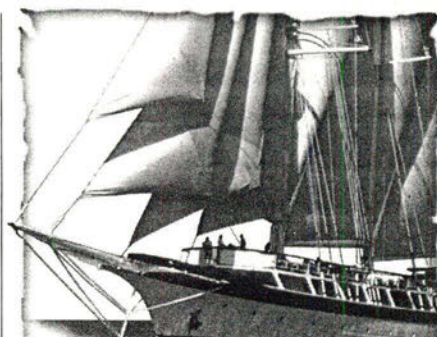
For the police, precise images mean a new investigative tool, says James Frelk, the vice-president of EarthWatch, the company that plans the first new satellite launch. Officers monitoring a suspected crack house, for example, will be able to see the pattern of vehicles arriving and leaving. "They can see the difference between a van, a truck, and a car," Frelk says, "and make a good guess about whether the same car was there yesterday." He expects local governments to be regular customers for other uses, such as updating tax assessments and spotting additions to homes and outbuildings that are in violation of building codes.

The Fourth Amendment to the Consti-

tution has traditionally been understood to protect homes and the areas immediately surrounding them from unreasonable government intrusion; laws of trespass have protected against snooping by businesses or individuals. In the days before electronic wizardry, that meant freedom from physical entry. When wiretapping and hidden microphones made intrusion possible without breaking down doors or climbing fences, the idea of privacy became more subjective. The Constitution was then taken to mean that areas where individuals have "a reasonable expectation of privacy," including homes and yards, must remain free of government intrusion—physical or electronic.

But in the past ten years judicial support for the use of aerial photography to spot marijuana crops in the war against drugs has left doubt about whether any outdoor space can be considered private. The last time the Supreme Court ruled on the question, in 1986, it upheld the legality of an aerial backyard search that produced pictures of a stand of marijuana plants, hidden from view on the ground by a ten-foot-high fence. In the war against drugs "one of the casualties has been the Fourth Amendment," says Yale Kamisar, a professor of constitutional law at the University of Michigan and a leading authority on privacy issues. Most constitutional scholars agree that increasingly sophisticated technology is no justification for lessening the protection of privacy in one's home and yard. Yet courts continue to uphold warrantless searches of yards by means of aerial surveillance, even though the searches would be illegal if the police jumped a fence. "We have much less privacy than we think," Kamisar says. "If the Fourth Amendment doesn't adapt to new technology, it's going to wither and die."

Corporate privacy, too, is shrinking. On the same day that it upheld the aerial search for marijuana plants, the Supreme Court ruled on a case in which inspectors from the Environmental Protection Agency sought entry without a warrant to the 2,000-acre Dow Chemical plant in Midland, Michigan, in order to check emissions from power plants and take photographs, and were denied it. The inspectors then rented a plane and took seventy-five color photos using an aerial mapping camera; the Court found that



Experience a Great Adventure!

Join us on a 6 or 13 day Caribbean expedition from \$650.

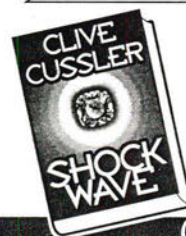
Call your travel agent for more information or 1-800-327-2601.

Windjammer Barefoot Cruises

P.O. Box 190120, Dept. 204, Miami Beach, FL 33119

BOOKS ON TAPE #1

World's Largest Selection



- Best Sellers on Cassette
- Full-length Readings
- Call for Free Brochure

(800) 626-3333

Box 7900-AT, Newport Beach, CA 92658

Reg. U.S. Pat. & T.M. Off.

PROVENCE BASQUE PYRENEES TUSCANY AND THE CINQUE TERRE

CLASSIC JOURNEYS

Easy going walking, cultural and natural history tours:

- expert local naturalist and historian guides
- historic and charming inns and lodges
- small groups

For a free color catalog call toll-free: 1-800-200-3887

SWISS ALPS SWISS AND ITALIAN LAKES COSTA RICA

NEW ZEALAND KENYA ITALY'S AMALFI COAST

Half Moon

Golf, Tennis & Beach Club

Montego Bay, Jamaica

See your travel agent or call 800-626-0592 • 809-953-2211

Member ERI/Heinz E. W. Simonitsch, Dir.

To drive more
confidently into
a future nobody
can predict, call
1-800-582-SAAB,
Ext. 200.

Some are content to watch as events unfold before them. But if you'd rather control your destiny, we suggest the Saab 9000 CS. Its 2.3-liter turbocharged engine will give you power on demand, and its superb handling provides quick response to any twists and turns that lie ahead. It also has a cavernous cargo space (56.4 cu. ft.). Which should provide enough room for whatever else the future holds.

Call for a free Saab Excursion Kit giving complete information on all our models. And the perfect Saab to find your own road.



The Saab Excursion Kit.

©1996 SAAB CARS USA, INC.
www.saabusa.com

inspection using aerial photography did not violate the Constitution.

Confusing matters further, the Court left clues that government satellite surveillance might be an invasion of privacy even when aerial photography is not. The majority said that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant." In each of the two cases four dissenting justices thought that there should be more protection of privacy than the Court provided.

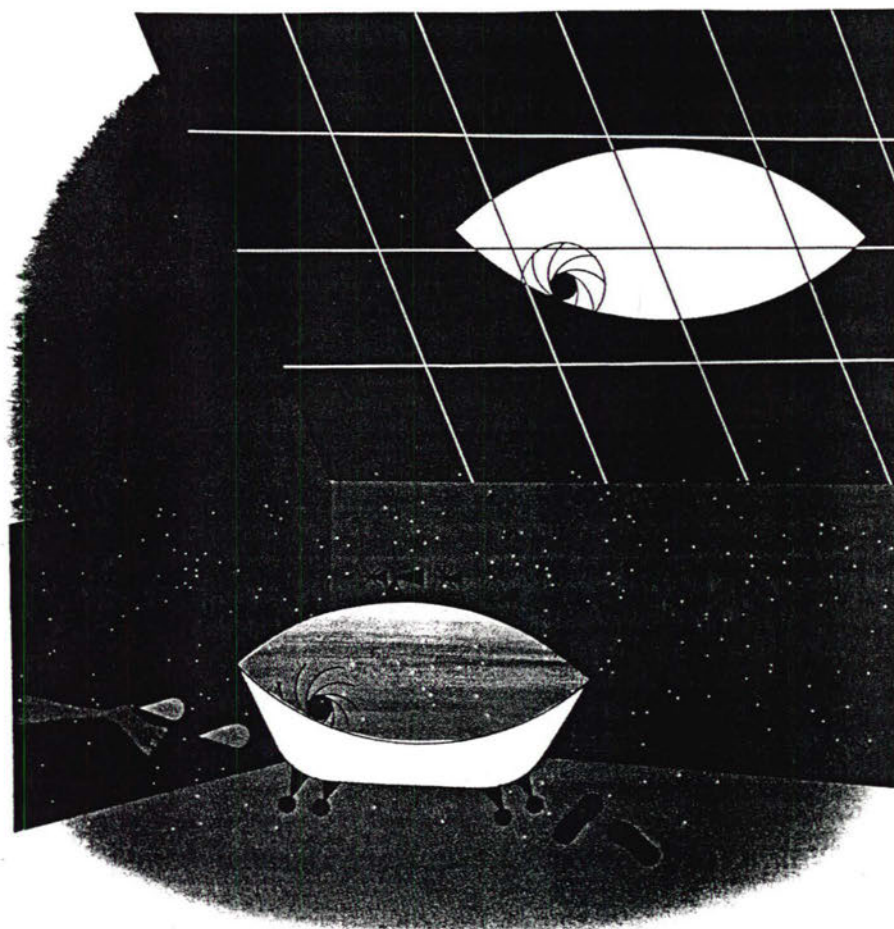
Other threats to privacy arise when scattered public information is combined with precise images of homes or farms. A new wing on a house, a trip to the Caribbean, and a few major purchases could together signal a change in lifestyle of interest to tax collectors, business partners, or ex-spouses. Farmers competing for high yields could profit from a week-by-week record of a neighbor's success in using irrigation, fertilizers, and pesticides. New satellites will make information accessible on personal computers within hours.

Congress and state legislatures have in some instances restricted the free flow of information among companies and between government agencies and companies. Self-restraint by businesses and government agencies, too, can go a long way toward avoiding consumers' worst nightmares. But advances in technology are running far ahead of efforts to limit their use. Any further privacy protection will have to be legislated. "Whenever privacy questions occur in the context of new technology, it takes a long time for the courts to respond," says Gilbert S. Merritt, the chief judge of the U.S. Court of Appeals for the Sixth Circuit, who wrote the appellate opinion upholding the EPA's aerial surveillance of the Dow Chemical plant. "The last issues arose with wiretapping. It's taken forty years to reach some kind of stability in that law."

MOST new information, of course, will not raise privacy questions. But on what terms will it be shared? Until now geographic data have been treated as a national resource. Only a few governments have been capable of

launching earth-observing satellites. The last generation of U.S. civilian satellites, the Landsat series, was financed by taxpayers, and most of its images are available to the public for the cost of duplicating the information. (Landsat images have been distributed commercially since 1985.) But the next group of earth-observing satellites is being financed and launched by private companies. Their images will be produced under contract, customized for clients, and made available at market prices. EarthWatch will retain the ownership of all its images, licensing their use by individual customers and restricting their reproduction, just as computer companies now limit the copying of software. Foreign governments, large corporations, and other paying clients will get exclusive rights to information they pay for—a big change. "Up to now, when we have acquired mapping information by contract, it has been in the public domain," says Gale TeSelle, who coordinates geographic data at the Department of Agriculture. "We give it away or we sell it as inexpensively as possible." TeSelle believes that by using such information to encourage farmers to fight erosion, for example, or to use a minimum of chemicals against pests, the government can "increase the conservation ethic."

None of these concerns should slow the next steps in mapping the earth. It is cause for celebration that we are entering a time of competitive, unpredictable exploration just when description of the seven continents seemed virtually complete. Amid budget pressures and privatization efforts, however, there is real danger that simple and familiar protections will be compromised. Whatever the public and commercial value of creating precise maps linking physical characteristics of residences with other publicly available information, the making of those maps should be limited by the traditional notion that a person's home and surrounding areas are private. And commercial satellite ventures should be limited by the idea that geographic information remains a national resource, to be shared at minimal cost. Dangers lie not in what satellite sensors can record but in how the political system allows that information to be used. The clearer the protections now, the greater the likely benefits later. ☼



High Resolution, Unresolved

Private companies will soon launch satellites powerful enough to spot environmental hazards—or a car in your driveway. Should we worry about snooping from space?

FOR more than thirty years spy satellites launched by the United States have been gathering a "virtual time-machine record of the earth," as Vice President Al Gore has described it. The public has paid close to \$100 billion for that record. But national-security and personal-privacy concerns

by **Mary Graham**

have blocked the use of the world's most powerful sensors to make current information about natural resources, environmental hazards, and private property in the United States available to environmental scientists, government agencies, and businesses. Because the Central Intelligence Agency is barred by

federal law from spying on Americans, it shares current environmental information about the United States only in rare instances—for example, in response to natural disasters.

Now, though, spy-satellite technology that has been used for a single purpose—espionage—with extraordinary government controls can suddenly be used for any purpose with few controls. In 1994, concerned about the post-Cold War health of the U.S. aerospace industry and fearful that foreign competition might challenge U.S. leadership in satellite technology, the Clinton Administration decided that private companies could launch satellites with high-resolution sensors previously available only to the intelligence community, and could provide information to anyone willing to pay for it. As government officials take cautious steps to share information gathered by military satellites, four U.S. companies are racing to launch satellites of their own equipped with similar technology. The first launch is scheduled for later this summer.

At a recent conference in Washington, D.C., Mark Brender, ABC's Pentagon producer, predicted that precise pictures from space will revolutionize television news, both by freeing reporters from relying on government-provided information during international crises and by freeing viewers from relying solely on what reporters tell them. David Bohrmann, an executive producer at NBC, demonstrated how networks could use satellite pictures to simulate flyovers of troop encampments in Bosnia. At his command a technician in New York using prerecorded images zoomed in on villages, scanned rivers, and hovered over military bases, producing a moving picture that resembled a helicopter ride around the countryside.

WHAT is really at stake is the ground rules for the next phase of mapping the earth. By next year three of the four companies plan to produce images of one-meter resolution—100 times as precise as those of current civilian satellites. The ability to see hazy outlines of large buildings will be replaced with the ability to see the clear shapes of small

cars. The ability to observe the same farm or city block every sixteen days will be replaced with the ability to observe the same point every two or three days; three to six images a day of most places in the United States are promised within four years.

Fundamental issues are being decided now. When should the government be allowed to censor images to protect national security? Should fears of military snooping from space be replaced with fears of snooping by corporations or domestic agencies? Will access to satellites' most detailed pictures pass from a small cadre of military clients with top-secret clearance to a small cadre of corporate clients with the means to pay for them?

Since commercial use of this technology is new, no one has a ready framework for resolving questions about national security, the protection of privacy, and public access to information. Time-tested principles that allow the government to block information in emergencies, keep homes and their surroundings free from intrusion, and treat geographic information as a national resource can provide guidance—if they are heeded. The breadth of the government's power to censor images may be decided this fall, when the Commerce Department is expected to issue final policies setting the conditions for commercial licenses to operate satellites. Privacy questions may be decided in an international context: strict privacy rules adopted by the European Union last July require consent for the use of information that identifies an individual. They may keep companies in the United States from selling images abroad unless similar rules are approved in this country. Access questions—whether images can be copied and distributed to the public, for example—will probably be negotiated between satellite companies and their customers, including government agencies.

NO longer simply the source of spectacular views of the earth, satellite images have a new capacity to influence what people do and how they think. Using sophisticated software and powerful, inexpensive computers, businesses, government agencies, citizens' groups, and individuals can now produce layered

maps (called Geographic Information Systems, or GIS) that combine new environmental findings with information already available to the public, such as property ownership and census data. New satellites will make such maps more useful by providing high-resolution images with digital precision and offering predictable repeat visits. Neither aerial photography nor current civilian satellites like Landsat or the French SPOT can produce this combination.

The investigative powers of satellites derive not just from photography but from sensors measuring visible and invisible wavelengths of the sun's energy. These can reveal more about an object's character than can be discovered standing next to it: each species of plant, type of soil, and kind of rock or building material, for example, uniquely reflects and absorbs wavelengths. Experts add a few caveats: measures of reliability are critical; interpretation is complicated; and much of this science is still in its infancy. And like all maps, these reflect the quality of underlying information.

Information from sensors can give early warning of environmental hazards. Kass Green, the president of Pacific Meridian Resources, a mapping firm, expects that new images will help minimize the damage done by wildfires like those that sweep through urban areas such as Los Angeles and Oakland, California. For the first time, she says, it will be possible to easily distinguish asphalt, wood-shake, and synthetic-shake roofs and to assess from week to week the dryness of vegetation around homes. Planning firebreaks and other preventive measures depends on accurately predicting a fire's path.

Satellite maps can help to settle political controversies—or create them. When, for example, environmental groups and the Bush Administration clashed over how much old-growth forest in the Pacific Northwest should be protected as habitat for the spotted owl, competing layered maps produced by the Wilderness Society and the federal Forest Service provided a basis for negotiation, by clarifying different ways of defining old growth. New maps of Latin America that were completed last fall by the World Wildlife Fund have led to a debate about how to use limited conservation funds: the maps make

clear that tropical dry forests and grasslands are as important to biodiversity as rain forests, and are more severely threatened.

Satellite images can make things harder to hide. The Environmental Protection Agency has used such images to help identify hazardous-waste sites and sources of water pollution. European farmers, who receive crop subsidies of \$50 billion a year, have new reasons to submit accurate information: their planting patterns are monitored from space by the European Commission. When farm boundaries are layered over images of the countryside, infrared color codes reveal whether a field is growing barley, wheat, corn, or something else.

OF course, newly explicit images can also be used to make mischief. Foreign intelligence agencies are expected to be among the largest buyers of high-resolution images. "International security issues are serious," says Ray Williamson, a senior research scientist at the George Washington University Space Policy Institute. "Iraq would be interested in information about Saudi Arabia. Iran would like to see data about Israel. India and Pakistan would like to have information about each other. If you were concerned about troop buildup on your border, you could put in a standing order for the satellite to take a picture every time it passed over." During international conflicts this greater access could lessen the information advantage the United States has over other countries.

Some experts argue that expanded access could be beneficial. Neighboring countries might be less quick to threaten each other when troop movements were visible to all: When U.S. troops are involved in international conflicts, though, the U.S. government has a strong interest in controlling the flow of information. "One reason we were able to best the Iraqis," Williamson says, "was that we had very good information about them and they didn't know what we were doing."

To minimize security risks, the U.S. government is working to keep "shutter control"—broad latitude to turn off sensors when images might compromise "national security, international obligations and/or foreign policies." Representatives of television networks and other

news media argue that the government's authority to stop the use of satellite images should be no broader than its authority to stop the publication or airing of other sensitive information, and that exercising it should require the same judicial process.

Whatever the outcome of that debate, growing international competition means that customers who want high-resolution images will probably be able to buy them. The CIA has been cautious about declassifying spy-satellite pictures: so far only archives from 1960 to 1972 have been released to the public, and the results of a joint U.S.-Russian effort to study environmentally important sites around the world using spy satellites will be kept secret for the foreseeable future. But Russia is already selling some current two-meter images from military satellites, and France, Israel, and Japan plan to market high-resolution imagery.

WHERE to draw the line between personal privacy and the public and commercial need for information will become urgent when high-resolution surveillance is routine. For the first time, detailed pictures of every piece of private property in the United States will be routinely compiled and marketed. Commercial satellites cannot yet produce images of people, but they can show vehicles parked in driveways and structural changes to homes. They can provide images within a few hours and exact comparisons of the same property at precise intervals without giving clues about their presence—things that aerial photography cannot do.

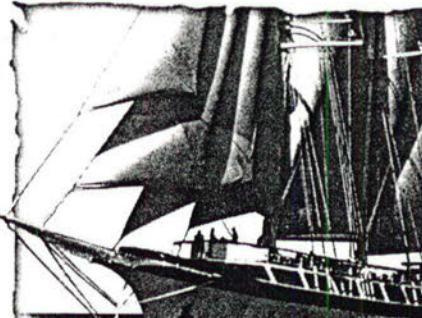
For the police, precise images mean a new investigative tool, says James Frelk, the vice-president of EarthWatch, the company that plans the first new satellite launch. Officers monitoring a suspected crack house, for example, will be able to see the pattern of vehicles arriving and leaving. "They can see the difference between a van, a truck, and a car," Frelk says, "and make a good guess about whether the same car was there yesterday." He expects local governments to be regular customers for other uses, such as updating tax assessments and spotting additions to homes and outbuildings that are in violation of building codes.

The Fourth Amendment to the Consti-

tution has traditionally been understood to protect homes and the areas immediately surrounding them from unreasonable government intrusion; laws of trespass have protected against snooping by businesses or individuals. In the days before electronic wizardry, that meant freedom from physical entry. When wiretapping and hidden microphones made intrusion possible without breaking down doors or climbing fences, the idea of privacy became more subjective. The Constitution was then taken to mean that areas where individuals have "a reasonable expectation of privacy," including homes and yards, must remain free of government intrusion—physical or electronic.

But in the past ten years judicial support for the use of aerial photography to spot marijuana crops in the war against drugs has left doubt about whether any outdoor space can be considered private. The last time the Supreme Court ruled on the question, in 1986, it upheld the legality of an aerial backyard search that produced pictures of a stand of marijuana plants, hidden from view on the ground by a ten-foot-high fence. In the war against drugs "one of the casualties has been the Fourth Amendment," says Yale Kamisar, a professor of constitutional law at the University of Michigan and a leading authority on privacy issues. Most constitutional scholars agree that increasingly sophisticated technology is no justification for lessening the protection of privacy in one's home and yard. Yet courts continue to uphold warrantless searches of yards by means of aerial surveillance, even though the searches would be illegal if the police jumped a fence. "We have much less privacy than we think," Kamisar says. "If the Fourth Amendment doesn't adapt to new technology, it's going to wither and die."

Corporate privacy, too, is shrinking. On the same day that it upheld the aerial search for marijuana plants, the Supreme Court ruled on a case in which inspectors from the Environmental Protection Agency sought entry without a warrant to the 2,000-acre Dow Chemical plant in Midland, Michigan, in order to check emissions from power plants and take photographs, and were denied it. The inspectors then rented a plane and took seventy-five color photos using an aerial mapping camera; the Court found that



Experience a Great Adventure!

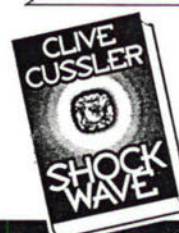
Join us on a 6 or 13 day Caribbean expedition from \$650.

Call your travel agent for more information or
1-800-327-2601.

Windjammer Barefoot Cruises
P.O. Box 190120, Dept. 204, Miami Beach, FL 33119

BOOKS #1 ON TAPE

World's Largest Selection



- Best Sellers on Cassette
- Full-length Readings
- Call for Free Brochure

(800) 626-3333

Box 7900-A1, Newport Beach, CA 92658

PROVENCE BASQUE PYRENEES TUSCANY AND THE CINQUE TERRE

CLASSIC JOURNEYS

Easy going walking, cultural and natural history tours:

- expert local naturalist and historian guides
- historic and charming inns and lodges
- small groups

For a free color catalog call toll-free:
1-800-200-3887

NEW ZEALAND KENYA SWISS ALPS SWISS AND ITALIAN LAKES COSTA RICA ITALY'S AMALFI COAST



Half Moon

Golf, Tennis & Beach Club

Montego Bay, Jamaica

See your travel agent or call
800-626-0592 • 809-953-2211

Member ERI/Heinz E. W. Simonitsch, Dir.

To drive more
confidently into
a future nobody
can predict, call
1-800-582-SAAB,
Ext. 200.

Some are content to watch as events unfold before them. But if you'd rather control your destiny, we suggest the Saab 9000 CS. Its 2.3-liter turbocharged engine will give you power on demand, and its superb handling provides quick response to any twists and turns that lie ahead. It also has a cavernous cargo space (56.4 cu. ft.). Which should provide enough room for whatever else the future holds.

Call for a free Saab Excursion Kit giving complete information on all our models. And the perfect Saab to find your own road.



The Saab Excursion Kit.

©1996 SAAB CARS USA, INC.
www.saabusa.com

inspection using aerial photography did not violate the Constitution.

Confusing matters further, the Court left clues that government satellite surveillance might be an invasion of privacy even when aerial photography is not. The majority said that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant." In each of the two cases four dissenting justices thought that there should be more protection of privacy than the Court provided.

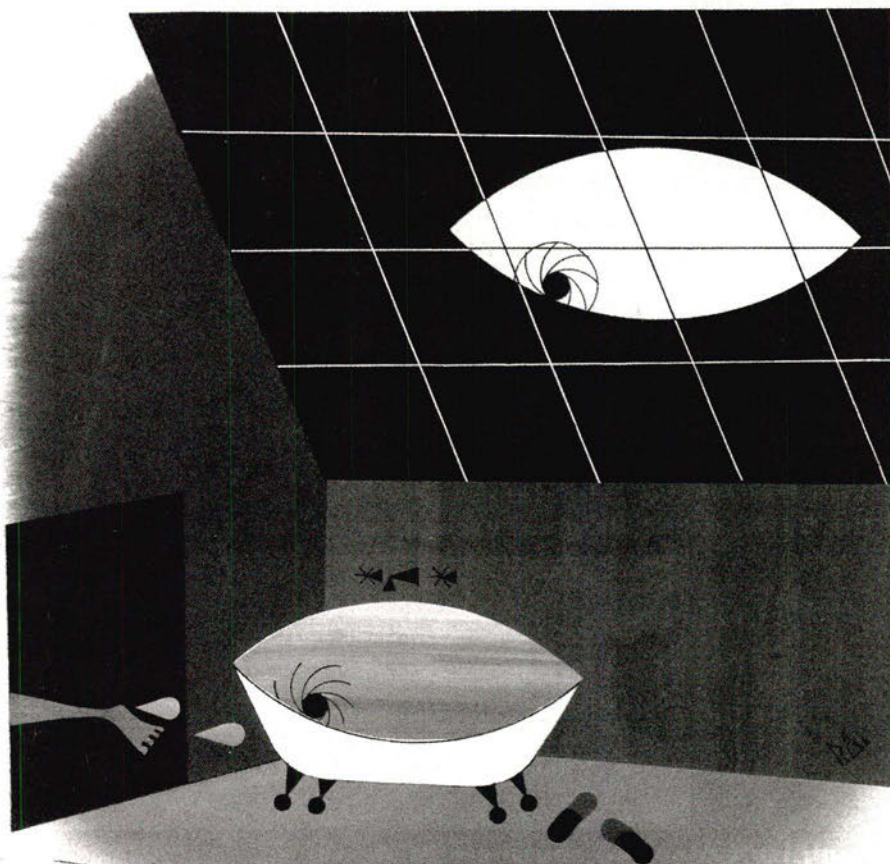
Other threats to privacy arise when scattered public information is combined with precise images of homes or farms. A new wing on a house, a trip to the Caribbean, and a few major purchases could together signal a change in lifestyle of interest to tax collectors, business partners, or ex-spouses. Farmers competing for high yields could profit from a week-by-week record of a neighbor's success in using irrigation, fertilizers, and pesticides. New satellites will make information accessible on personal computers within hours.

Congress and state legislatures have in some instances restricted the free flow of information among companies and between government agencies and companies. Self-restraint by businesses and government agencies, too, can go a long way toward avoiding consumers' worst nightmares. But advances in technology are running far ahead of efforts to limit their use. Any further privacy protection will have to be legislated. "Whenever privacy questions occur in the context of new technology, it takes a long time for the courts to respond," says Gilbert S. Merritt, the chief judge of the U.S. Court of Appeals for the Sixth Circuit, who wrote the appellate opinion upholding the EPA's aerial surveillance of the Dow Chemical plant. "The last issues arose with wiretapping. It's taken forty years to reach some kind of stability in that law."

MOST new information, of course, will not raise privacy questions. But on what terms will it be shared? Until now geographic data have been treated as a national resource. Only a few governments have been capable of

launching earth-observing satellites. The last generation of U.S. civilian satellites, the Landsat series, was financed by taxpayers, and most of its images are available to the public for the cost of duplicating the information. (Landsat images have been distributed commercially since 1985.) But the next group of earth-observing satellites is being financed and launched by private companies. Their images will be produced under contract, customized for clients, and made available at market prices. EarthWatch will retain the ownership of all its images, licensing their use by individual customers and restricting their reproduction, just as computer companies now limit the copying of software. Foreign governments, large corporations, and other paying clients will get exclusive rights to information they pay for—a big change. "Up to now, when we have acquired mapping information by contract, it has been in the public domain," says Gale TeSelle, who coordinates geographic data at the Department of Agriculture. "We give it away or we sell it as inexpensively as possible." TeSelle believes that by using such information to encourage farmers to fight erosion, for example, or to use a minimum of chemicals against pests, the government can "increase the conservation ethic."

None of these concerns should slow the next steps in mapping the earth. It is cause for celebration that we are entering a time of competitive, unpredictable exploration just when description of the seven continents seemed virtually complete. Amid budget pressures and privatization efforts, however, there is real danger that simple and familiar protections will be compromised. Whatever the public and commercial value of creating precise maps linking physical characteristics of residences with other publicly available information, the making of those maps should be limited by the traditional notion that a person's home and surrounding areas are private. And commercial satellite ventures should be limited by the idea that geographic information remains a national resource, to be shared at minimal cost. Dangers lie not in what satellite sensors can record but in how the political system allows that information to be used. The clearer the protections now, the greater the likely benefits later. ☛



High Resolution, Unresolved

Private companies will soon launch satellites powerful enough to spot environmental hazards—or a car in your driveway. Should we worry about snooping from space?

FOR more than thirty years spy satellites launched by the United States have been gathering a “virtual time-machine record of the earth,” as Vice President Al Gore has described it. The public has paid close to \$100 billion for that record. But national-security and personal-privacy concerns

by **Mary Graham**

have blocked the use of the world’s most powerful sensors to make current information about natural resources, environmental hazards, and private property in the United States available to environmental scientists, government agencies, and businesses. Because the Central Intelligence Agency is barred by

federal law from spying on Americans, it shares current environmental information about the United States only in rare instances—for example, in response to natural disasters.

Now, though, spy-satellite technology that has been used for a single purpose—espionage—with extraordinary government controls can suddenly be used for any purpose with few controls. In 1994, concerned about the post-Cold War health of the U.S. aerospace industry and fearful that foreign competition might challenge U.S. leadership in satellite technology, the Clinton Administration decided that private companies could launch satellites with high-resolution sensors previously available only to the intelligence community, and could provide information to anyone willing to pay for it. As government officials take cautious steps to share information gathered by military satellites, four U.S. companies are racing to launch satellites of their own equipped with similar technology. The first launch is scheduled for later this summer.

At a recent conference in Washington, D.C., Mark Brender, ABC’s Pentagon producer, predicted that precise pictures from space will revolutionize television news, both by freeing reporters from relying on government-provided information during international crises and by freeing viewers from relying solely on what reporters tell them. David Bohrmann, an executive producer at NBC, demonstrated how networks could use satellite pictures to simulate flyovers of troop encampments in Bosnia. At his command a technician in New York using prerecorded images zoomed in on villages, scanned rivers, and hovered over military bases, producing a moving picture that resembled a helicopter ride around the countryside.

WHAT is really at stake is the ground rules for the next phase of mapping the earth. By next year three of the four companies plan to produce images of one-meter resolution—100 times as precise as those of current civilian satellites. The ability to see hazy outlines of large buildings will be replaced with the ability to see the clear shapes of small

cars. The ability to observe the same farm or city block every sixteen days will be replaced with the ability to observe the same point every two or three days; three to six images a day of most places in the United States are promised within four years.

Fundamental issues are being decided now. When should the government be allowed to censor images to protect national security? Should fears of military snooping from space be replaced with fears of snooping by corporations or domestic agencies? Will access to satellites' most detailed pictures pass from a small cadre of military clients with top-secret clearance to a small cadre of corporate clients with the means to pay for them?

Since commercial use of this technology is new, no one has a ready framework for resolving questions about national security, the protection of privacy, and public access to information. Time-tested principles that allow the government to block information in emergencies, keep homes and their surroundings free from intrusion, and treat geographic information as a national resource can provide guidance—if they are heeded. The breadth of the government's power to censor images may be decided this fall, when the Commerce Department is expected to issue final policies setting the conditions for commercial licenses to operate satellites. Privacy questions may be decided in an international context: strict privacy rules adopted by the European Union last July require consent for the use of information that identifies an individual. They may keep companies in the United States from selling images abroad unless similar rules are approved in this country. Access questions—whether images can be copied and distributed to the public, for example—will probably be negotiated between satellite companies and their customers, including government agencies.

NO longer simply the source of spectacular views of the earth, satellite images have a new capacity to influence what people do and how they think. Using sophisticated software and powerful, inexpensive computers, businesses, government agencies, citizens' groups, and individuals can now produce layered

maps (called Geographic Information Systems, or GIS) that combine new environmental findings with information already available to the public, such as property ownership and census data. New satellites will make such maps more useful by providing high-resolution images with digital precision and offering predictable repeat visits. Neither aerial photography nor current civilian satellites like Landsat or the French SPOT can produce this combination.

The investigative powers of satellites derive not just from photography but from sensors measuring visible and invisible wavelengths of the sun's energy. These can reveal more about an object's character than can be discovered standing next to it: each species of plant, type of soil, and kind of rock or building material, for example, uniquely reflects and absorbs wavelengths. Experts add a few caveats: measures of reliability are critical; interpretation is complicated; and much of this science is still in its infancy. And like all maps, these reflect the quality of underlying information.

Information from sensors can give early warning of environmental hazards. Kass Green, the president of Pacific Meridian Resources, a mapping firm, expects that new images will help minimize the damage done by wildfires like those that sweep through urban areas such as Los Angeles and Oakland, California. For the first time, she says, it will be possible to easily distinguish asphalt, wood-shake, and synthetic-shake roofs and to assess from week to week the dryness of vegetation around homes. Planning firebreaks and other preventive measures depends on accurately predicting a fire's path.

Satellite maps can help to settle political controversies—or create them. When, for example, environmental groups and the Bush Administration clashed over how much old-growth forest in the Pacific Northwest should be protected as habitat for the spotted owl, competing layered maps produced by the Wilderness Society and the federal Forest Service provided a basis for negotiation, by clarifying different ways of defining old growth. New maps of Latin America that were completed last fall by the World Wildlife Fund have led to a debate about how to use limited conservation funds: the maps make

clear that tropical dry forests and grasslands are as important to biodiversity as rain forests, and are more severely threatened.

Satellite images can make things harder to hide. The Environmental Protection Agency has used such images to help identify hazardous-waste sites and sources of water pollution. European farmers, who receive crop subsidies of \$50 billion a year, have new reasons to submit accurate information: their planting patterns are monitored from space by the European Commission. When farm boundaries are layered over images of the countryside, infrared color codes reveal whether a field is growing barley, wheat, corn, or something else.

OF course, newly explicit images can also be used to make mischief. Foreign intelligence agencies are expected to be among the largest buyers of high-resolution images. "International security issues are serious," says Ray Williamson, a senior research scientist at the George Washington University Space Policy Institute. "Iraq would be interested in information about Saudi Arabia. Iran would like to see data about Israel. India and Pakistan would like to have information about each other. If you were concerned about troop buildup on your border, you could put in a standing order for the satellite to take a picture every time it passed over." During international conflicts this greater access could lessen the information advantage the United States has over other countries.

Some experts argue that expanded access could be beneficial. Neighboring countries might be less quick to threaten each other when troop movements were visible to all. When U.S. troops are involved in international conflicts, though, the U.S. government has a strong interest in controlling the flow of information. "One reason we were able to best the Iraqis," Williamson says, "was that we had very good information about them and they didn't know what we were doing."

To minimize security risks, the U.S. government is working to keep "shutter control"—broad latitude to turn off sensors when images might compromise "national security, international obligations and/or foreign policies." Representatives of television networks and other

news media argue that the government's authority to stop the use of satellite images should be no broader than its authority to stop the publication or airing of other sensitive information, and that exercising it should require the same judicial process.

Whatever the outcome of that debate, growing international competition means that customers who want high-resolution images will probably be able to buy them. The CIA has been cautious about declassifying spy-satellite pictures: so far only archives from 1960 to 1972 have been released to the public, and the results of a joint U.S.-Russian effort to study environmentally important sites around the world using spy satellites will be kept secret for the foreseeable future. But Russia is already selling some current two-meter images from military satellites, and France, Israel, and Japan plan to market high-resolution imagery.

WHERE to draw the line between personal privacy and the public and commercial need for information will become urgent when high-resolution surveillance is routine. For the first time, detailed pictures of every piece of private property in the United States will be routinely compiled and marketed. Commercial satellites cannot yet produce images of people, but they can show vehicles parked in driveways and structural changes to homes. They can provide images within a few hours and exact comparisons of the same property at precise intervals without giving clues about their presence—things that aerial photography cannot do.

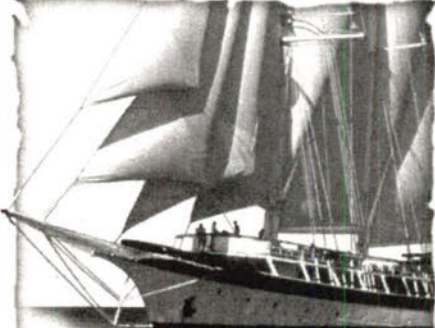
For the police, precise images mean a new investigative tool, says James Frelk, the vice-president of EarthWatch, the company that plans the first new satellite launch. Officers monitoring a suspected crack house, for example, will be able to see the pattern of vehicles arriving and leaving. "They can see the difference between a van, a truck, and a car," Frelk says, "and make a good guess about whether the same car was there yesterday." He expects local governments to be regular customers for other uses, such as updating tax assessments and spotting additions to homes and outbuildings that are in violation of building codes.

The Fourth Amendment to the Consti-

tution has traditionally been understood to protect homes and the areas immediately surrounding them from unreasonable government intrusion; laws of trespass have protected against snooping by businesses or individuals. In the days before electronic wizardry, that meant freedom from physical entry. When wiretapping and hidden microphones made intrusion possible without breaking down doors or climbing fences, the idea of privacy became more subjective. The Constitution was then taken to mean that areas where individuals have "a reasonable expectation of privacy," including homes and yards, must remain free of government intrusion—physical or electronic.

But in the past ten years judicial support for the use of aerial photography to spot marijuana crops in the war against drugs has left doubt about whether any outdoor space can be considered private. The last time the Supreme Court ruled on the question, in 1986, it upheld the legality of an aerial backyard search that produced pictures of a stand of marijuana plants, hidden from view on the ground by a ten-foot-high fence. In the war against drugs "one of the casualties has been the Fourth Amendment," says Yale Kamisar, a professor of constitutional law at the University of Michigan and a leading authority on privacy issues. Most constitutional scholars agree that increasingly sophisticated technology is no justification for lessening the protection of privacy in one's home and yard. Yet courts continue to uphold warrantless searches of yards by means of aerial surveillance, even though the searches would be illegal if the police jumped a fence. "We have much less privacy than we think," Kamisar says. "If the Fourth Amendment doesn't adapt to new technology, it's going to wither and die."

Corporate privacy, too, is shrinking. On the same day that it upheld the aerial search for marijuana plants, the Supreme Court ruled on a case in which inspectors from the Environmental Protection Agency sought entry without a warrant to the 2,000-acre Dow Chemical plant in Midland, Michigan, in order to check emissions from power plants and take photographs, and were denied it. The inspectors then rented a plane and took seventy-five color photos using an aerial mapping camera; the Court found that



Experience a Great Adventure!

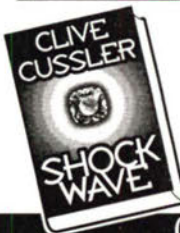
Join us on a 6 or 13 day Caribbean expedition from \$650.

Call your travel agent for more information or 1-800-327-2601.

Windjammer Barefoot Cruises
P.O. Box 190120, Dept. 204, Miami Beach, FL 33119

BOOKS #1 ON TAPE

World's Largest Selection



- Best Sellers on Cassette
- Full-length Readings
- Call for Free Brochure

(800) 626-3333

Box 7900-AT, Newport Beach, CA 92658

PROVENCE BASQUE PYRENEES TUSCANY AND THE CINQUE TERRE

CLASSIC JOURNEYS

Easy going walking, cultural and natural history tours:

- expert local naturalist and historian guides
- historic and charming inns and lodges • small groups

For a free color catalog call toll-free:
1-800-200-3887

NEW ZEALAND KENYA SWISS ALPS SWISS AND ITALIAN LAKES COSTA RICA ITALY'S AMALFI COAST



Half Moon

Half Moon's Beach Club
Montego Bay, Jamaica

See your travel agent or call
800-626-0592 • 809-953-2211

Member ERI/Heinz E. W. Simonitsch, Dir.

To drive more
confidently into
a future nobody
can predict, call
1-800-582-SAAB,
Ext. 200.

Some are content to watch as events unfold before them. But if you'd rather control your destiny, we suggest the Saab 9000 CS. Its 2.3-liter turbocharged engine will give you power on demand, and its superb handling provides quick response to any twists and turns that lie ahead. It also has a cavernous cargo space (56.4 cu. ft.). Which should provide enough room for whatever else the future holds.

Call for a free Saab Excursion Kit giving complete information on all our models. And the perfect Saab to find your own road.



The Saab Excursion Kit.

©1996 SAAB CARS USA, INC.
www.saabusa.com

inspection using aerial photography did not violate the Constitution.

Confusing matters further, the Court left clues that government satellite surveillance might be an invasion of privacy even when aerial photography is not. The majority said that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant." In each of the two cases four dissenting justices thought that there should be more protection of privacy than the Court provided.

Other threats to privacy arise when scattered public information is combined with precise images of homes or farms. A new wing on a house, a trip to the Caribbean, and a few major purchases could together signal a change in lifestyle of interest to tax collectors, business partners, or ex-spouses. Farmers competing for high yields could profit from a week-by-week record of a neighbor's success in using irrigation, fertilizers, and pesticides. New satellites will make information accessible on personal computers within hours.

Congress and state legislatures have in some instances restricted the free flow of information among companies and between government agencies and companies. Self-restraint by businesses and government agencies, too, can go a long way toward avoiding consumers' worst nightmares. But advances in technology are running far ahead of efforts to limit their use. Any further privacy protection will have to be legislated. "Whenever privacy questions occur in the context of new technology, it takes a long time for the courts to respond," says Gilbert S. Merritt, the chief judge of the U.S. Court of Appeals for the Sixth Circuit, who wrote the appellate opinion upholding the EPA's aerial surveillance of the Dow Chemical plant. "The last issues arose with wiretapping. It's taken forty years to reach some kind of stability in that law."

MOST new information, of course, will not raise privacy questions. But on what terms will it be shared? Until now geographic data have been treated as a national resource. Only a few governments have been capable of

launching earth-observing satellites. The last generation of U.S. civilian satellites, the Landsat series, was financed by taxpayers, and most of its images are available to the public for the cost of duplicating the information. (Landsat images have been distributed commercially since 1985.) But the next group of earth-observing satellites is being financed and launched by private companies. Their images will be produced under contract, customized for clients, and made available at market prices. EarthWatch will retain the ownership of all its images, licensing their use by individual customers and restricting their reproduction, just as computer companies now limit the copying of software. Foreign governments, large corporations, and other paying clients will get exclusive rights to information they pay for—a big change. "Up to now, when we have acquired mapping information by contract, it has been in the public domain," says Gale TeSelle, who coordinates geographic data at the Department of Agriculture. "We give it away or we sell it as inexpensively as possible." TeSelle believes that by using such information to encourage farmers to fight erosion, for example, or to use a minimum of chemicals against pests, the government can "increase the conservation ethic."

None of these concerns should slow the next steps in mapping the earth. It is cause for celebration that we are entering a time of competitive, unpredictable exploration just when description of the seven continents seemed virtually complete. Amid budget pressures and privatization efforts, however, there is real danger that simple and familiar protections will be compromised. Whatever the public and commercial value of creating precise maps linking physical characteristics of residences with other publicly available information, the making of those maps should be limited by the traditional notion that a person's home and surrounding areas are private. And commercial satellite ventures should be limited by the idea that geographic information remains a national resource, to be shared at minimal cost. Dangers lie not in what satellite sensors can record but in how the political system allows that information to be used. The clearer the protections now, the greater the likely benefits later. ☪

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

27-Sep-1996 06:27pm

TO: Timothy J. Brennan

FROM: Nancy E. Schwartz
Office of Mgmt and Budget, IAD

SUBJECT: FTC Suggests Expanding Personal Data Protection In Credit

FTC Suggests Expanding Personal Data Protection In Credit Reporting Act
The Federal Trade Commission is recommending amendments to the Fair Credit Reporting Act to extend the statute's confidentiality protections to a broader range of personal data, including identifying information such as a person's social security number, the maiden name of the consumer's mother, prior addresses, and date of birth.

Such information -- now available through certain electronic databases -- could be used to "facilitate identity fraud, credit fraud, and other illegal activities," FTC Chairman Robert Pitofsky said in a Sept. 20 letter to Sen. Richard Bryan (D-Nev), the ranking minority member of the Senate Banking Subcommittee on Financial Institutions and Regulatory Relief.

The FTC's move follows press reports that personal information about millions of Americans is available for a fee from Lexis-Nexis through its new "P-Trak" on-line database. While Lexis-Nexis says it ceased dissemination of social security numbers in June, a user can still obtain other identifying information about a person by providing the person's social security number. The P-Trak database reportedly is fed by a credit bureau that maintains information, including identifying information, about individuals for the purpose of generating consumer reports. According to Pitofsky, the FTC "has received numerous complaints and Congressional inquiries concerning" services such as P-Trak.

The fraud and illegal activities that one armed with this information can pursue "may outweigh the limited legitimate uses of this information for locating individuals," Pitofsky told Bryan.

In August, the FTC met with credit bureau representatives, creditors, law enforcement personnel, consumer groups, and other interested parties and discovered how the information available on such a service can help fraud artists "open credit lines in innocent consumers' names and run up unpaid charges, thereby ruining the consumers' credit histories," the FTC chief said.

Proposed Amendments

The FCRA protects the privacy of consumer reports compiled by credit bureaus by restricting access to such information. However, it currently does not prohibit the disclosure of identifying information about a consumer that is not credit-related.

Accordingly, the FTC is proposing amendments to the FCRA that would expand the definition of consumer report under Section 603(d) to include "any communication by a consumer reporting agency of any identifying information

other than the consumer's name, generational designation, current address and telephone number."

Pitofsky told Bryan that Congress should consider amending Section 602 -- the act's "findings and purpose" provision -- to reflect the need for consumer reporting agencies to exercise their responsibilities with "concern for the confidentiality of consumer information."

Likewise, Section 602(b) should reflect the act's mandate that consumer reporting agencies utilize information, "including identifying information," pursuant to the act's requirements, the FTC chairman said.

In a Sept. 23 press release, the FTC advised consumers to reconcile billing statements with their credit card accounts each month, as they would their checking account. Any questionable charges should be reported promptly to the card issuer, it added.

In addition, if they so desire, consumers "could investigate how to remove their names from publicly available lists," the FTC advised. Financial Institutions