structural integrity on sinking, submarines get badly broken. On passing their design depth, they implode and the hull either breaks at that point or is gravely weakened. The submarine then accelerates downward, crashing into the sea bottom at sometimes remarkable speeds. The *Thresher*, for example, is held by some estimates to have impacted at a speed of 100 knots (115 miles per hour). Others, however, believe that 25 to 30 knots is the maximum descent speed a sinking sub can attain.

Whatever its exact impact velocity, the structure is almost certain to break up, if the accidents with American submarines are anything to go by. According to Captain William Walker, an engineer in the Office of the Oceanographer of the Navy, the *Scorpion* lies with its bow and stern ends broken off, although the midship section is fairly intact. The *Thresher* broke into a greater number of pieces and is surrounded by a field of debris about half a mile in radius. Asked about the apparent raising of the Soviet submarine in one piece Walker said: "That was quite remarkable to me considering our experience with the *Thresher* and *Scorpion*. I would have expected at least the bow and stern sections to have been fractured off."

If the submarine was indeed in one piece, it is hard to reconcile such figures as have been published with the magnitude of the operation required. The Russian submarine is reported to belong to a category, the Golf class, which has a displacement weight of 2800 tons. Estimates obtained by *Science* for the submarine's likely deadweight range from 2000 to 8000 tons, and several newspapers cite a figure of 4000 tons. But the lifting capacity of the *Glomar Explorer* is usually quoted as 800 tons, attributed either to the ship's main derrick or its submersible barge, which is clearly insufficient to raise an entire submarine.

Almost all accounts mention that a drill pipe with a large claw at the end was used to raise the submarine. (*Time*, in its diagram, shows four cables, but its text describes the use of piping.) According to the Los Angeles *Times*, the *Glomar Explorer*'s drill pipe had walls 4 inches thick with a hollow core 3 inches in diameter. Rough calculation suggests that a drill pipe of these dimensions, if made of the strongest steel used in commercially available drill pipes, could lift some 3400 tons before it started to deform. If the submarine weighed 4000 tons, it is hard to see how the Los Angeles *Times*' drill pipe could have lifted it in one piece.

Rumor in the ocean mining world, however, has it that the drill pipe was a massive 16 inches in diameter. Both this and the figures quoted above are reconciled in the version given by a mining engineer close to one of the contractors for the *Glomar Explorer*. The engineer, who declines to be identified, says that the ship used different thicknesses of pipe to construct a tapered drill string, with the pipe at the top having walls as thick as 6 inches. He states that the *Glomar Explorer*'s derrick had a total lifting capacity of about 5000 tons. If its drill string weighed 1500 tons, the ship would have a lifting capacity of 3500 tons with which to overcome suction effects and raise its payload. Another mining engineer, John Miro of Ocean Resources Inc., San Diego, believes that ship may have used steel cables to assist the drill pipe.

It is hard to distinguish whether a lifting capacity of this order would have been designed to lift the whole submarine, or just a single large fragment of it. (If the Russian submarine broke into three pieces, like the *Scorpion*, with its midships intact, this section might amount to a large fraction of its total tonnage.)

If the submarine was indeed in pieces, it would have been much easier to salvage, and has quite possibly been retrieved in its entirety. If, on the other hand, the *Glomar Explorer* succeeded in lifting the entire submarine, as the semi-official version claims, the ship should have little trouble in recovering the two thirds which dropped back, especially since the second descent of the stricken submarine would almost certainly shatter it into easily retrievable fragments.—NICHOLAS WADE

Privacy: Congressional Efforts Are Coming to Fruition

The issue of privacy is finally having its day in Congress. The last Congress (93rd) saw the introduction of scores of bills designed to protect individuals from surveillance and record-keeping activity of government and government-funded agencies.

Two of them passed. One was the so-called Buckley amendment to the Elementary and Secondary Education Amendments of 1974, which increases access to student records by students and their parents, and inhibits it for others. The other, more far-reaching law represents the first attempt to set government-wide standards regulating data banks containing records on individuals held by most agencies in the federal government. Called the Privacy Act of 1974, it is the final legacy of Senator Sam J. Ervin (D–N.C.) who retired from Congress last December. The law goes into effect on 27 September.

These two measures are the early blossomings of what promises to be an entirely new family of legislation designed to stem the real or potential erosion of personal liberty caused by massive and promiscuous data collection, use, and dissemination by all levels of government as well as the private sector.

The Privacy Act is couched in fairly general terms—what it does is articulate a set of principles to ensure that information is only used for the purpose for which it was collected and to let members of the public know what the government knows about them. It lays a basis for future, more specific legislation governing the handling of various categories of information. The law is actually one of the federal government's first steps in building a theoretical framework for achieving a balance, in both the public and private sectors, between the individual's right to privacy and society's "need to know." The latter concept is already formalized in the Freedom of Information Act; one intended effect of the privacy measure is to clarify one of the exemptions in the FOI act that prohibits the dispensation of information when that involves a clearly unwarranted invasion of privacy.

There is a fair amount of stabbing in the dark involved in privacy legislation, and it is case law that will eventually determine its substance. Meanwhile, as Ruth M. Davis, director of the Institute for Computer Sciences and Technology at the National Bureau of Standards, observes, one inevitable spinoff will be the development and revival of good information management practices. (NBS has been deeply involved in developing standards for confidentiality and security in automated data systems.) The government has been in possession of files it didn't even know about, as was revealed in a 3-year study completed in 1974 by the Ervin subcommittee of the Senate Judiciary Committee. That study found 858 data banks in 54 agencies, all of which contained more than 1.25 billion files on individuals. The Privacy Act

POINT OF VIEW

Stamp Out Food Faddism

Food faddism is indeed a serious problem. But we have to recognize that the guru of food faddism is not Adelle Davis, but Betty Crocker. The true food faddists are not those who eat raw broccoli, wheat germ, and yogurt, but those who start the day on Breakfast Squares, gulp down bottle after bottle of soda pop, and snack on candy and Twinkies.

Food faddism is promoted from birth. Sugar is a major ingredient in baby food desserts. Then come the artifically flavored and colored breakfast cereals loaded with sugar, followed by soda pop and hot dogs. Meat marbled with fat and alcoholic beverages dominate the diets of many middle-aged people. And, of course, white bread is standard fare throughout life.

This diet—high in fat, sugar, cholesterol, and refined grains—is the prescription for illness; it can contribute to obesity, tooth decay, heart disease, intestinal cancer, and diabetes. And these diseases are, in fact, America's major health problems. So if any diet should be considered faddist, it is the standard one. Our far-out diet—almost 20 percent refined sugar and 45 percent fat—is new to human experience and foreign to all other animal life. . . .

It is incredible that people who eat a junk food diet constitute the norm, while individuals whose diets resemble those of our great-grandparents are labeled deviants. . . .—*From an editorial in* Nutrition Action, *March-April 1975, a newsletter of the Center for Science in the Public Interest, Washington, D.C.*

should make it more difficult to maintain the large number of obsolete, redundant, or unnecessary files that number would seem to imply.

Over the years, legal scholars have attempted to define privacy—one of the earliest is Louis D. Brandeis's formulation of it in 1890 as "the right to be let alone." A later formulation by Alan F. Westin of Columbia University is that privacy is "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about themselves is communicated to others." Privacy is not defined by the Constitution, although the preponderance of legal opinion has it that the right to privacy is implicit in the Bill of Rights.

Since the substance of privacy cannot be strictly defined, Congress has chosen instead to establish procedures which enable individuals to take measures to protect what they perceive to be their privacy.

The 1974 act is the first federal statute to establish this right. How did it finally get through? Considerable public interest became focused on the subject during a long-running series of hearings held by former Representative Cornelius Gallagher's (D–N.J.) select privacy committee during the 1960's. One development that brought attention to bear on privacy was a proposal by the then Bureau of the Budget to set up a centralized, automated National Data Bank. The idea was that efficiency would be served by pooling the files of such mammoth information-holders as the Internal Revenue Service, the Social Security Administration, and the Census Bureau. It seemed like a good idea until critics pointed up the unsavory, not to mention frightening, implications of thousands of bureaucrats having fingertip access to cradle-to-grave information on millions of Americans. The proposal was quashed.

The civil disorders and law-and-order ethos of the 1960's probably slowed the march of privacy legislation, but as citizens found themselves increasingly numbered and coded and categorized—not just criminals and poor people, but ordinary types who minded their own business—the image of the country being taken over by a heedless army of computers has come even closer to the surface of public consciousness. Watergate greatly increased the sense of urgency. Ironically enough, with Watergate in high tide, Nixon gave his new vice president Gerald Ford the go-ahead to chair a new Committee on the Right of Privacy within the White House Domestic Council. Official history has it that Ford was a little nonplussed by the investigative procedures that preceded his appointment as vice president and developed a permanent personal interest in privacy matters. His successor, Nelson Rockefeller, has not displayed any notable involvement in the committee's activities, but the committee, directed by former management consultant executive Douglas Metz, has by all accounts done an admirable job working with Congress and generally giving the privacy issue high-level visibility and support. In Congress, a coalition of two usually divergent factions—the conservatives and the civil libertarians—has created a base broad enough to boost privacy proposals into law. In the Senate this has been exemplified by Ervin and Roman Hruska (R–Neb.) joining forces; in the House, by the coauthorship of several privacy bills by liberal Edward I. Koch (D–N.Y.) and conservative Barry Goldwater, Jr. (R–Calif.).

The Privacy Act was originally framed to cover information-handling practices by state and local governments and private industry as well as the federal government. It was subsequently pared down to apply only to the federal government, and even there large areas—notably criminal justice information systems—are left out. But it does set down unprecedented principles that will presumably be drawn upon in the creation of future privacy laws at every level of government.

The principles are taken from a proposed code of fair information practices contained in a 1973 report called "Records, computers, and the rights of citizens" put together by the Advisory Committee on Automated Personal Data Systems of the Department of Health, Education, and Welfare. That report asserted that there must be no personal data record-keeping systems whose very existence is secret; that individuals must be allowed to find out what's in their files and to cause erroneous information to be corrected; that agencies should make clear the purposes of their data systems; and that information collected for one purpose must not be used for another without the consent of the data subject.

The Privacy Act requires that all federal agencies publish annual reports on the nature of all their personal data-keeping systems and obtain permission for expansion of data systems or creation of new ones. Interagency transfer of information is tightly restricted except for what is called "routine use" (defined in the law as "compatible with the purpose for which it was collected"). The law sets up a Privacy Protection Study Commission to monitor enforcement of the statute [which is administered by the Office of Management and Budget (OMB)] and to study issues that will have to be dealt with in the future. It will study, for example, the spread of the use of the social security number for purposes unrelated to social security—a phenomenon that, while convenient for record keepers, makes it easier for various files on an individual to be integrated with each other.

The law is vague—the OMB has issued a 114-page document of guidelines for its implementation—and it will probably take several years and countless court cases to define its substance and workability. One reason for the vagueness is that it is more of a preventive or anticipatory measure than one to curtail specific abuses. It is

easy to collect horror stories involving misuse of private information—but the most pervasive abuses are more subtle, more difficult to track down, and often perpetrated by agencies whose intentions are of the best.

No one really knows how expensive it will be to implement the new law, although a Senate staffer says the OMB's estimate of $200 million to $300 million a year is a gross exaggeration, particularly in light of the fact that some savings are bound to be effected by the correction of sloppy information handling practices.

The next generation of congressional privacy legislation is now being designed to fill in the gaps left by the Privacy Act and to develop rules, by subject area, for information systems operated or funded by the federal government.

Most important on this year's agenda is a law to regulate the handling of criminal justice information by the federal government and all state and local law enforcement agencies that get federal funds. The House and Senate judiciary committees now have two bills under consideration, one authored by the Administration and one masterminded by Ervin. There is general agreement that criminal justice files are pretty much in disarray. On the federal level, it is difficult to place restrictions on information management because the Federal Bureau of Investigation (FBI) doesn't want any rules—such as sealing criminal histories or expunging arrest records after a specified period of time—that would cramp pursuit of its mission. The problems are legion. Lack of accuracy and completeness of records is one of the worst. It is estimated, for example, that of the arrest records held by the FBI's National Crime Information Center (a data bank in which states voluntarily participate), 70 percent contain no information on the final disposition of the cases. The spread of automation has allowed for easy and indiscriminate circulation of arrest records (whether or not followed by conviction) and unverified data. What's more, prospective employers, credit agencies, and other non-law enforcement bodies are given access to individual criminal records. The bills pending are designed to limit the use of incomplete records, to keep criminal justice information within the system, and to inhibit direct access of one system into another. And, in keeping with the Privacy Act (into which the final measure is supposed to plug), subjects of criminal files would have the opportunity to inspect and demand correction of their files.

There are quite a few other privacy bills simmering along in various committees governing use of Internal Revenue Service files, government personnel files, medical files, banking and savings and loan files, military surveillance, and so on.

Senator William Proxmire (D-Wis.) intends to introduce amendments to the Fair Credit Reporting Act. That act, passed in 1970, was the government's pioneer effort at giving individuals some control over personal information by requiring that consumer credit agencies tell them what is in their files. The act is now deemed inadequate, and provisions are being drawn up that would enable people to see their files in person, uncover specific reasons why they were rejected for credit, learn the identity of their "accusers," and take legal action on broader grounds than those allowed in the original act.

There is also a bill, introduced by Koch and Goldwater and named, appropriately enough, H.R.1984, that would apply, to data banks held by local governments and the private sector, the same principles that the Privacy Act establishes for those within the federal government. The Administration thinks such a measure would be premature, and many private businesses contend that specific abuses should be identified before the government starts tinkering with their information systems. There certainly would seem to be a need to sharpen up definitions. What, for example, is a personal file? What, for that matter, is a data bank? Some people fear that such a law could even put restrictions on the maintenance of newspaper morgues or company correspondence files. Anyway, H.R.1984's chance of passage, at least in its present form, is extremely remote.

It may be that the states will take the responsibility for laws governing privacy in the private sector. Several states, including Massachusetts, California, and Hawaii, are developing laws governing their own data systems; farthest along is Minnesota, which now has a law governing data banks containing personal information held by all states and state-funded agencies. Some private organizations are moving ahead on their own—IBM, for example, has developed new measures to limit the scope of information required for employee files, and is advertising principles it has adopted to give employees access to their own records and limit access by third parties. If the trend continues, privacy practices could become formally embodied in the structures of large organizations in the way equal employment opportunity functions have been.

A new family of privacy legislation will mean a new family of trade-offs. The most fundamental question relates to the amount of information the government needs on individuals in order to protect the well-being of society. If future laws put limits on the amount, type, retention, and use of information collected from individuals, there will inevitably be new impediments to efficient rendering of government services, law enforcement, and the availability of data for statistical and research purposes. Balanced against these drawbacks will be not only the indefinable "right to privacy" but also the feeling of freedom and security that enables citizens to exercise their constitutional rights without looking over their shoulders all the time.—CONSTANCE HOLDEN

NIH: Reunion Held to Boost Morale and Gain Political Visibility

On Monday, 21 April, the nominations of Theodore Cooper to be assistant secretary for health in the Department of Health, Education, and Welfare (HEW) and Donald S. Fredrickson to be director of the National Institutes of Health (NIH) finally became official when President Ford sent their names to the Senate for confirmation. Within 2 weeks, routine confirmation hearings were held and now, after several months of waiting, it looks as though the biomedical community will have leaders in Washington.

Washington has been the scene of an unusual amount of activity involving the biomedical world lately. On the weekend preceding the formal Cooper-Fredrickson nominations, NIH held a party, a reunion that lured more than 700 nostalgic alumni to its campus just outside of the Capital. The following weekend, NIH held an open house for the public, an estimated 25,000 to 30,000 of whom showed up to tour laboratories and watch science movies. On