Reflections on the Sixtieth Anniversary of the Communications Act

Senator Carol Moseley-Braun *

"They could plug in your wire whenever they wanted to. You had to live-did live, from habit that became instinct-in the assumption that every sound you made was overheard, and, except in the darkness, every moment scrutinized."(note 1)

In the literary classic *1984*, George Orwell warned of a society where one's every move was monitored; a society where nothing was private or sacred. "Big Brother," the watchful eye of the government, peered down over everything and everyone, knew the citizenry's innermost thoughts, and destroyed their very spirits.

As we move toward the twenty-first century, Orwell's vision of the future-a future devoid of privacy-is increasingly nearer to reality. Contrary to Orwell's forecast, however, the greatest threat to individual privacy comes not from the government, but from technology in the private sector. Through the use of computer databases and direct-mail marketing lists, individuals and companies throughout the country have access to some of the most intimate and detailed personal information that, if asked, you might decline to give to anyone. The failure of the government to draft comprehensive privacy legislation has greatly contributed to this growing problem.

An example of a typical day which illuminates the issue recently appeared in the *Los Angeles Times*. You drive to work along the highway, where toll booths electronically register which cars are passing by, and park at the garage across from your office, under the watchful eye of the garage's security camera. When you arrive at work, your employer reads your electronic mail messages, listens in on your phone conversations, and records progress on your computer by registering the number of key strokes you hit per minute, or by viewing the actual document you are working on. Of course, your employer has already accessed insurance company databases to retrieve detailed information on your health background and credit databases to uncover your personal financial history.

After lunch-which you bought with a credit card, thereby creating a permanent record of your dining tastes that will be sold to direct marketers-you stop at the ATM, where the machine records how much money you withdrew, while a hidden security camera takes your picture. The cash you withdrew is used to buy groceries at the local supermarket, where the cashier scans your electronic discount card, allowing the store to compile a detailed record of your shopping preferences.

Finally, upon arriving home, you call a clothing store catalog and order merchandise with your credit card. Again, the retailer and credit card company compile detailed information on your likes and dislikes. Of course, let us not forget that the phone company makes a record of every phone number you have called and the duration of that call.(note 2) That is just a typical day in the life of the average American. It is not fiction, but today's reality.

Numerous examples exist to demonstrate just how widespread the decline of privacy has become. To cite just one, a recent survey of 301 businesses found that 22 percent of the companies surveyed had searched employees' computer files, voice mail, e-mail, and other electronic data systems. Those percentages were even higher among larger corporations.(note 3) While I could cite many other examples, this one demonstrates that, while Orwell was right about the erosion of personal privacy, he was wrong about the government being the only source of danger to our privacy. The truth is that, while we have to be on guard against governmental actions that undermine our right to privacy, we also need government to help protect us from nongovernmental erosion of that fundamental right.

Some individuals, particularly those who make the profits, see no danger in the collection of such "innocuous" private data. I disagree. Consider the words of Professor Paul Schwartz, a noted expert on privacy regulation, "Personal information, when disclosed to family and friends, helps form the basis of trust; in the hands of strangers, this

information can have a corrosive effect on individual autonomy."(note 4)

Protection of individual autonomy has far reaching implications. In the past twenty years, battles over the right to privacy have focused primarily on reproductive freedom and a woman's right to choose. In fact, the terms "right to privacy" and "right to choose" have become virtually synonymous.

However, while reproductive freedom is certainly one important area of individual freedom, the right of privacy encompasses much more. As Justice Louis Brandeis stated in his now-famous dissent:

> The makers of our constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men.(note 5)

There are, of course, competing views over where the "right to privacy" contained in the Constitution is found. Justice Blackmun wrote in *Roe v. Wade* that the Fourteenth Amendment's concept of ordered liberty and restrictions on state action implied a right to privacy.(note 6) Justice Goldberg stated in a concurring opinion in *Griswold v. Connecticut*: "The Ninth Amendment shows a belief of the Constitution's authors that fundamental rights exist that are not expressly enumerated in the first eight amendments and an intent that the list of rights included there not be deemed exhaustive."(note 7) Others have argued that the right to privacy is contained in the Tenth Amendment's reservation of powers for the state, the Fourth Amendment's protection from unreasonable searches and seizures, or the Third Amendment's prohibition on forcing individuals to house soldiers in their home. But the pressing question facing those of us in Congress is not necessarily where the right to privacy arises. Rather, it is how we protect that right in light of advancing communications.

Technology is increasing at such a rapid pace in this country that our laws simply have not caught up. Twenty years ago, Congress created the United States Privacy Protection Study Commission to conduct an extensive examination of privacy in the information age. Few, if any, of its recommendations have actually been implemented. We tend to be so enthusiastic about the capabilities of the new technology-the novelty of paying our bills over the phone or sending instantaneous electronic mail messages across the continents-that we forget to examine the underlying implications of the technology. The few laws governing data protection that exist today are ad hoc protections enacted to address unique concerns specific to one industry or another, but they do not provide the kind of general, comprehensive protection that many Americans desire. As we embrace emerging communications technologies, therefore, we must work to ensure that privacy concerns are given as much weight as concerns about commerce and regulation.

For example, consider the issue of privacy of medical records. Much like the principle of lawyer-client confidentiality, each patient has an expectation that information given to his or her physician will stay with his or her physician, or will be distributed only to those who have an absolute need to know. Without such expectations, the intimacy of the doctor-patient relationship could become meaningless. Who would be completely honest with their physician-who would admit they had a drug problem or previously had an abortion or had been exposed to the virus that causes AIDS-if they knew that information would be accessible to their employer or their next-door neighbor? Yet such information is vital if a physician is to properly treat a patient. If our health care system cannot adequately guarantee privacy, then it may provide substantial disincentives for Americans to speak honestly with their doctors, a result that could seriously undermine individual treatment and the public health. Despite this, there are virtually no federal laws regulating the confidentiality of medical records.

By way of contrast, in 1987, when a list of videos rented by Robert Bork was made public during his ultimately unsuccessful confirmation hearings, disclosure of video rental information was made illegal.(note 8) This example demonstrates the absurdity that can result from ad hoc privacy policymaking. Medical records, containing the most intimate and private information imaginable, do not receive as much protection as the movies checked out from Blockbuster last Friday. Anyone who doubts how painful this discrepancy is need only check with the family of the late Arthur Ashe, whose medical records indicating he was afflicted with HIV, the virus that causes AIDS, were made

public long before he and his family were ready to disclose this information. As more and more health information is stored "on-line," the problem can only get worse. Clearly, a consistent legislative policy in this area is long overdue.

The development of a policy to address this problem cannot happen overnight. Sale of personal information has ballooned into a multi-billion dollar industry, one that is certain to resist regulatory efforts. But without basic guarantees of privacy, the information superhighway may be as risky as a narrow two-lane mountain road without guardrails. Logging on to a nameless, faceless network can be a very risky activity without the right kind of assurance that the information voluntarily given out will be used only by the person to whom it was given, and only for the purpose for which it was provided. It is up to Congress to provide these assurances. And Congress is beginning to do just that.

Sen. Patrick Leahy (D-Vt.) has introduced S. 2129, a bill that will establish guidelines for protected health information and provide for criminal penalties for those who release such information.(note 9) Sen. Paul Simon (D-Ill.) has introduced S. 1735, the Privacy Protection Act of 1993, which would establish a Privacy Protection Commission to provide guidance to the federal government in the areas of privacy and data protection.(note 10) The Commission would be able to recommend model standards and guidelines for federal, state, and local agencies to follow in carrying out current privacy protections, as well as to recommend to Congress any necessary legislative changes. In addition, Sen. Simon's bill to prevent abuses of electronic monitoring will outline in what context, and to what extent, employers may monitor their workers.(note 11)

The Telephone Privacy Act of 1993, introduced by Sen. Bumpers (D-Ark.), would require telephone companies that offer caller ID (a service that displays the phone number of the person calling before the phone has been answered) to give callers the option of per call blocking.(note 12) The option would allow consumers to block display of their telephone numbers on a per call basis without an extra charge. Sen. Murray (D-Wash.) has proposed a bill that will direct the Secretary of Commerce to study the issue of exportation of encryption technology, currently prohibited, that will allow American companies overseas to safeguard the same level of privacy that is currently enjoyed by companies on American soil.(note 13)

The fact underscored by each of these bills is that Congress can no longer afford to ignore the privacy implications of pending legislation. The communications and computer revolutions have made it possible to compile huge amounts of information and to access it almost instantaneously. However, our ability to handle all of this information with due concern for people's privacy has not kept pace with technological advancements. The future offers many exciting opportunities, but it also offers real dangers if we fail to protect our privacy. As we move forward, privacy must receive a more heightened level of protection. After all, if the freedoms we possess as Americans do not encompass the right to control the information we disseminate about ourselves, and to whom we disseminate it, then how free are we?

****

Notes

*D-Ill. B.A. University of Illinois at Chicago; J.D. University of Chicago. Return to text

1. George Orwell, 1984, at 2 (Harcourt Brace Jovanovich 1977). Return to text

2. Thomas B. Rosenstiel, *Someone May Be Watching*, L.A. Times, May 18, 1994, at A1. Return to text

3. *Snooping at Work: Electronic Privacy in the Workplace Remains a Fuzzy Area*, Cleveland Plain Dealer, Jan. 16, 1994, at E1. Return to text

4. Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 Hastings L.J. 1321, 1322 (1992). Return to text

5. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Return to text

6. *Roe*, 410 U.S. 13, 153 (1973). Return to text

7. *Griswold*, 381 U.S. 479, 492 (1965) (Goldberg, J., concurring). Return to text

8. *See* Video Privacy Protection Act of 1988, Pub. L. No. 99-508, 100 Stat. 1860 (codified at 18 U.S.C. 2701 (1988)). Return to text

9. S. 2129, 103d Cong., 2d Sess. (1994). Return to text

10. S. 1735, 103d Cong., 1st Sess. (1993). Return to text

11. S. 984, 103d Cong., 1st Sess. (1993). Return to text

12. S. 311, 103d Cong., 1st Sess. (1993). Return to text

13. S. 2203, 103d Cong., 2d Sess. (1994). Return to text