The uses of modern technology present a challenge to constitutional rights. Computer technology is viewed as a serious threat to privacy, electronic bugging devices are available to everyone, and the United States government is the largest user of electronic surveillance. The fact that databases are pervasive is evidenced by the realization that the U.S. government has three billion personal computer files that are sources of potential exploitation. Is it possible for the 200-year-old U.S. Constitution to adapt to the new technology? Can courts and laws change rapidly enough to protect citizens from what is now technologically possible? A social studies lesson plan presents three issues for classroom use: (1) changes in technology are accompanied by changes in the social institutions; (2) technology makes possible new threats to basic freedoms; and (3) there is constant tension between what technology makes possible and what should be allowed when more than one basic freedom is threatened. Suggestions are provided for classroom activities that encourage discussion of the social implications of technological change. (NL)
SCIENCE, TECHNOLOGY AND THE CONSTITUTION:
A NEVER ENDING TENSION

Gerald W. Marker
Indiana University
Bloomington, Indiana

A paper delivered at the 67th Annual Meeting
of the National Council for the Social Studies
November, 1987
Dallas, Texas

Running head: The Constitution & Privacy
The concept of change is at the very heart of social studies. History is, in fact, a detailing of change over time, while the social sciences all view change as a major variable in their attempts to explain human behavior.

Change has always been a part of human history; but the pace of that change has itself changed. For countless generations the pace of change was so slow that the world of one generation was much like that of its parents. Cultures were modified as the need arose, but the changes were gradual. When horses were domesticated or the wheel invented, society adjusted to those new ways of doing things. But major as they were, such changes were few and far between.

Gradual change is no longer a part of our reality. The airplane has been with us for less than a century; television for less than fifty years! There are people still among us who remember what it was like to live without electricity and to travel by horse. Technology now is changing so rapidly that by the time a device goes on sale it is already obsolete. Society plays catch-up as it tries
to adjust its institutions to accommodate technologies which, for example, enable us to have host parents, birth control pills, genetic engineering, robots and artificial organs. The resulting tension between social institutions and new technology is so great that a new science-technology-society curriculum movement has emerged to try to bridge the mis-match between the three components. (1)

Of particular interest in this paper is the relationship between technology-driven, rapid change and some of the basic rights guaranteed in the Constitution. As we celebrate the survival of the Constitution for these past 200 years we should not take its survival for the next 200 years for granted. The principle of "adapt or die" is as true of our Constitution as it is of all social institutions.

Students often marvel at the simplicity of the U.S. Constitution. Those who wrote the document could hardly have foreseen the world in which we now apply it and it is to their credit that they found a way to protect our basic freedoms and establish a form of government which still endures. But technology is testing Constitutional adaptability as never before. The central focus of this paper are the challenges to Constitutional adaptability being posed by one area of rapid, technology-driven change which threatens our privacy.
Privacy: A Basic Right

Article IV of the Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Supreme Court Justice Louis D. Brandeis described privacy as, "...the right to be left alone--the most comprehensive of rights and the right most valued by civilized men."(2) Some might wish to argue that privacy is not the most comprehensive of rights but it may be one of the rights which is becoming the most difficult to preserve.

To the men who wrote the Constitution, privacy probably meant not having one's home or business entered without cause, or the right of having one's mail delivered intact. In a recent issue of TIME devoted to the Constitution the authors described what they believed were early views of privacy:

To the extent that Americans of 1787 thought about privacy, they conceived of it in terms of property, not individuals. Society was based on property, and restrictions on its acquisition or retention were
resisted. Bans on undue government searches were common in the states. But it was assumed that society could enforce shared norms of morality, either through laws or simply through meddling. Obscenity, blasphemy, adultery were all restricted. Anyone who did not like the community's values were still free to do as he pleased, but only by exercising his freedom to move on. (3)

Later, when the telephone was invented, privacy expanded to include the right to have secure conversations even though technology made wire taps possible. Privacy also meant, in practical terms, the privacy of one's records and the privacy of one's movements.

When people felt that their right to privacy had been invaded by something like an unreasonable search of their property they had recourse to the courts. Indeed, over the years the courts have expanded the meanings of basic rights such as the right to be free from unreasonable searches. For example, the MAPP RULE requires the exclusion of relevant evidence of guilt where that evidence was obtained in violation of the criminal's expectation of privacy. MIRANDA (1966) limits the authority of law enforcement officers to interrogate a suspect, i.e., to invade his or her privacy. (4)

The invention of the micro-chip started a process which may have a profound impact upon 4th amendment rights in general and privacy rights in particular. Many experts on privacy now consider "...computers a more serious threat to
privacy than any other technological development of the 20th century."\(^{(5)}\) Arthur Buskin, who worked on privacy issues in the Carter Administration, sees technology related to three major threats to privacy in the areas of eavesdropping, privacy of records, and surveillance.\(^{(6)}\) The situation is further complicated by the fact that present day technology makes it possible to invade the privacy of another without that person ever knowing that his or her privacy has been electronically compromised. Thus, new technology calls for new interpretations of Constitutional guarantees. Should, for example, the transmissions of data enjoy the same constitutional protection that is currently given to human speech? A few examples will illustrate the complexity of such a question.

Law enforcement officials have used wiretaps and surveillance to apprehend criminals. At the same time, the courts have placed strict limits on the use of such evidence gathering techniques. But what about those persons outside law enforcement who, for a variety of reasons, want to gather their own information? Obtaining the technology to engage in such activities is hardly a problem. In almost any electronics stores one can buy electronic bugging devices, some for as little as $19.95. Electronic mail-order houses, like Information Unlimited in New Hampshire, sell a sophisticated line of devices like a tiny
bug which can be plugged into a phone receiver to turn the earpiece of the phone into a microphone that can pick up conversations anywhere in the room. The device can be activated by dialing the phone number AND THE PHONE DOES NOT EVEN RING!

But the fact remains that one of the largest users of electronic surveillance is the government. Recently the Office of Technology Assessment surveyed 142 federal agencies (excluding foreign intelligence and counter intelligence) and identified 35 agencies that use or were planning to use electronic surveillance. (7)

At the next higher level of sophistication, equipment now exists which can unscramble the radio waves which are emitted by every computer. The problem has gotten so serious that the government is now designing standards which will limit the amount of such emissions which computers can exhibit. The Defense Department has already taken steps to shield the emissions of its computers from unwanted ears. Meanwhile, business people now worry whether competitors are listening to their computer talk and governments are probably listening to the computer emissions of other governments, including friendly ones. (8)
Listening in on the computer emissions of others is one facet of a broader and rapidly growing problem area. When communications flowed through wires, protecting privacy was one thing. Increasingly messages are sent via microwave transmissions, sometimes via satellites. Once "out in the open" such transmissions become difficult to protect. For example, because other countries are busy listening to transmissions such as overseas telephone calls, the National Security Administration also listens to those transmissions to make certain that sensitive information is controlled. NSA's master computers scan such transmissions for key words such as "Iran" or "Khoemini." When this practice was challenged in 1982, a U.S. Appeals Court decided that it was not illegal for the government to monitor such transmissions. (9)

Surprising as it may seem, electronic eavesdropping is not the greatest threat to privacy. Rather, it is the large and growing number of data bases which contain details about our daily lives. Such data bases are everywhere. The government alone maintains over 3 billion personal computer files. (10) Any person may find his or her name in data bases maintained by law enforcement agencies, license bureaus, state revenue agencies, banks, credit associations, credit card companies, electronic mail companies, cable TV companies, insurance companies, mail order houses, the
Internal Revenue Service, car rental agencies, hotels, hospitals, and the Social Security Administration. The list is almost endless. There are even companies which build computer databases from public records as diverse and seemingly harmless as telephone directories, vehicle registrations, voter registration lists, and ownership records, and certificates of birth, marriage, and death. Through a process called profiling the computer searches for persons with characteristics of special interest to companies. Such records are then sold to companies which want to market their products and services to particular segments of society, e.g., people who within the past year purchased an expensive automobile or took out health insurance.

Data bases will grow even more rapidly if predictions about where events are headed turn out to be accurate. One prediction is that in the future, rather than carry a deck of credit cards, consumers will carry one "smart card" which will include a computer chip memory device which will contain information about their bank account, health insurance, credit rating, medical record, employment status, etc. But, each time the card is used an electronic record of the transaction will be fed into one or more data bases, leaving electronic tracks for others to follow.
Such data bases are large, very large. The Internal Revenue Service files contain information about many millions of taxpayers. The law enforcement data base in California contains over two million records, can be accessed from 3,000 terminals, and was called upon to furnish information 1.3 million times in a three month period recently. (11)

Such enormous data bases are ripe for exploitation. The temptation to cross check the data in them is simply too strong to resist. For example, computer bank records can be used to determine if a person is eligible for welfare. The names of applicants for public works jobs can be compared to those in the criminal record data bases. Pay TV records can be used to locate potential child pornographers. The Selective Service System cross-checked draft registration lists with files maintained by the Social Security Administration and motor vehicle records to locate young men who had failed to register for the draft. The Department of Health and Human Services matched Social Security rolls with Medicare patients known to have died and discovered that checks were still being mailed to 8,000 dead people, and many of those checks were being cashed. Removing those names from the Social Security rolls saved the government $50 million and led to the conviction of 500 people. But, in the process of identifying these 8,000 people the computer
searched the files of 30 million innocent people. (12)
Meanwhile, such matching programs continue to increase in number. Over the last five years, federal computer matching programs have tripled in number, involving about 2 billion different records. (13)

Many Americans falsely assume that records containing their names are protected by the guarantees of the 4th amendment. The truth can be shocking. In 1976, in a case involving bank records which had been used to convict a Georgia bootlegger, the Supreme Court concluded that:

...the Fourth Amendment protection against unreasonable searches and seizures can't prevent a bank or other private organization from giving customer information to the government, even if that information initially was disclosed in confidence. (14)

In April of that same year Justice Lewis F. Powell, Jr., said that depositors run the risk that information they give to financial institutions will be "...conveyed...to the government." (15) Your boss, spouse, or credit agency could track your movements with the use of electronic banking records. No federal law bars banks from releasing this information to third parties. And bank records are not the only at-risk records. Law enforcement officers might be able to use electronic mail records to read messages you had sent. Unlike U.S. Postal Service mail, electronic mail is not protected from unauthorized search. Two-way cable TV subscribers could find that opinions they had registered
were being sold to interest groups such as political parties, along with their names and addresses. (16)

But humans are creative, and once they have access to high speed computers and millions of bits of information there is no limit to how such data can be employed. And there is more to come. It will soon be possible to measure the brain waves of workers and for computers (and employers) to monitor that data to determine levels of concentration and alertness. Used properly, such a system could save lives. Pilots, air traffic controllers, nuclear plant control room operators and other similar "crucial" occupations seem to offer settings for the reasonable application of such technologies. But that same technology could be used by any employer to monitor the brain waves of all employees in all situations, posing yet another threat to our beleaguered privacy and the Constitution which protects it.

The challenge to our system is two fold. First, can a Constitution drafted 200 years ago once again demonstrate its adaptability as it is interpreted in the light of these new technologies? Second, can our courts and laws change rapidly enough to protect us from what is now technologically possible? Arthur Buskin, a former Commerce
Department information policy official, cautions that "these technological advances happen so quickly that the normal process our government and society uses for adjusting to change does not have time to take effect." (17)

Privacy and the Curriculum

The previous portion of this paper focused upon how recent technological advances are providing new threats to our privacy, a set of rights broadly guaranteed by the 4th Amendment to the Constitution. This section of the paper will deal with lessons to be learned from this set of developments, lessons which are appropriate for social studies.

There are at least three lessons contained in the current concern over what is happening to our right to privacy.

LESSON # 1

Changes in technology are accompanied by changes in the social institutions in which they are embedded. Since social institutions require time to adjust there is seldom an early "fit" between them and the new technology. Finally, the more rapid the change in technology the longer the lag before the social system can adjust and thus to worse the "fit."
LESSON # 2

Technology makes possible new threats to the basic freedoms guaranteed by the Constitution. The judicial system must continually adapt interpretations of Constitutional intent as it applies to new technologies.

LESSON # 3

There is a constant tension between what technology makes possible and what should be allowed when more than one basic freedom is threatened.

Each of these lessons is appropriate for inclusion in the social studies curriculum.

The first lesson is the broadest of the three. It is a typical theme of science-technology-society courses and applies virtually to any society and to any time period. Sara Anderson has suggested an approach which students can use when they study past technological innovations.

1. List all the effects you can think of for one technological innovation introduced into our culture during the past 85 years.

2. Categorize the effects on your list according to whether they were planned and/or foreseen by those who introduced or eagerly adopted the innovation or were unplanned or unforeseen.

3. Indicate which effects were felt only in a local area, which were felt regionally, nationally and globally.
4. Divide the effects on your list into those you consider "positive," that is benefitting people in general and "negative," that is those which were harmful.

5. ...list four factors you consider essential to a good quality environment for human beings, and which influenced your choices in item # 4.

6. Which subgroups in society benefitted most from the innovation you are assessing? Which subgroups of society bear (or did bear) the majority of the burdens of the negative effects? List two reasons for the inequitable distribution of benefit and burden.

7. What was the time lapse between (a) the scientific or technological discovery which made the innovation possible and its widespread introduction or adoption? (b) between the planned benefits and the appearance and/or awareness of the burdens?

8. (a) What actions have been/are being taken to alleviate the burdens? (b) Who (government, industry, consumers) are taking these actions? (c) Who is paying the cost of alleviating these burdens in money? (d) Who is paying the cost of alleviating these burdens in Quality of Life?

9. What areas of CHOICE did the innovation open up for individuals?

10. What choices did the innovation open up for society in general (seen most likely in legislative and judicial decisions)?

While these questions would be appropriate for probing the impact of technology in general (and computers in particular) on our right to privacy, they could as appropriately be applied to innovations like the automobile or gunpowder. When the questions are applied to a significant innovation students will see that the micro-chip was not unique when it produced both "positive" and
"negative" effects, when it produced unanticipated consequences (what Robert Hanvey has called "surprise effects" (19)), when it benefited some segments of society more than others, when it opened a whole new range of choices, when it required new laws and social conventions to govern its use. In that sense, the invasions of privacy made possible by modern electronics will become just another example of the social implications of technology, of how society is in a constant state of change as social institutions adapt to the realities of new technology.

Lesson two has a narrower focus than lesson one. It raises a new set of questions for students (and judges) to consider. For example, should the transmission of data enjoy the same 4th Amendment protections which now apply to voice and written communications? Should any citizen have the right to purchase electronic eavesdropping or surveillance equipment? Once communications and data enter the public airways do they lose their personal nature and become public property? How far should individuals be allowed to go in claiming ownership of information and records relating to them? Is there a limit to what can and should be protected by the basic freedoms guaranteed by the 4th Amendment?

Instructionally, students can be confronted with the same dilemmas as judges as they try to interpret the
Constitution in light of new technology. Some may argue that students lack the sophisticated knowledge of judges, but one need only reflect on the current turmoil relating to a woman's right to have an abortion or to be a host mother to realize that the courts can lead but not ignore the broader society.

Lesson three deals with a matter of priorities. The Constitution guarantees our freedom from illegal searches, but most Americans also believe that they have a right to be safe in their homes and workplaces, to travel the highways without fear of drunk drivers, to have schools free from drugs. Often one widely held value is protected at the expense of another widely held value. The people must continue to answer the question, what price should citizens pay for safety and security? When are the rights of the group more important than the rights of the individual?

Developments in technology constantly redefine these vexing issues. For example, police roadblocks set up to catch drunk drivers might be viewed as illegal if they require blood tests and pose a major inconvenience for drivers. But what happens when technology provides us with a sobriety reading as soon as a motorist rolls down the car window to speak to the police officer? Does the technology now make roadblocks an acceptable search in 4th Amendment terms? To take the illustration one step further, what
happens when engineers develop an automobile ignition device which senses when the driver has had too much to drink and automatically keeps the engine from starting? At that point is the government, in the name of the greater social good, justified in requiring such a device be installed on all new cars or would such a requirement constitute an invasion of an individual's right to not be subjected to unreasonable searches?

The basic and delicate balance between conflicting "rights" is never settled. Technology is forever altering the mix of factors which must go into a consideration of this basic question.

Summary

The amazing thing about our Constitution is that it has endured for 200 years during which science and technology have drastically altered our social world. The courts must reinterpret Constitutional protections in terms of what is possible, given the new technology. The process of judicial reinterpretation is a part of a larger social adjustment process which must go on as social institutions shift to deal with the new technology. This adjustment process is complicated by the fact that the pace of technological change is increasing, compressing the adjustment process.
The impact of new technology on privacy rights is an excellent case study of this process.

END NOTES

1. For example, see Hickman, et. al., SCIENCE/TECHNOLOGY/SOCIETY: A FRAMEWORK FOR CURRICULUM REFORM IN SECONDARY SCHOOL SOCIAL SCIENCE AND SOCIAL STUDIES and the S/T/S GUIDELINES published by the National Council for the Social Studies. The Opposing Viewpoints SOURCES series recently added a volume titled SCIENCE AND TECHNOLOGY to its ten volume set.


3. Elmer-Dewitt, "Don't tread on my data: protecting individual privacy in the information age," TIME, p. 84.


6. Ibid.


8. Broad, "Government trying to silence leaky computers that tell all," FORT LAUDERDALE NEWS/SENTINEL.


10. "Civil liberties......," op. cit.


13. Elmer-DeWitt, "Don't tread on my data: protecting individual privacy in the information age," TIME, p. 84.


15. Ibid.


19. Hanvey, AN ATTAINABLE GLOBAL PERSPECTIVE.

REFERENCES

Broad, William J., "Government trying to silence leaky computers that tell all," FORT LAUDERDALE NEWS/SENTINEL, (Fort Lauderdale, Florida), April 17, 1983, p. 6F.


Grier, Peter, "Automatic tellers, electronic mail raise," CHRISTIAN SCIENCE MONITOR, April 19, 1984, pp. 3-4.

----, "That's not a picture hook--it's a 'bug'," CHRISTIAN SCIENCE MONITOR, April 16, 1984, pp. 1 & 33.

----, "Who's snooping and how? US and USSR 'peer into the mist'," CHRISTIAN SCIENCE MONITOR, April 17, 1984, p. 3.

----, "Wiretaps: is there enough supervision?" CHRISTIAN SCIENCE MONITOR, APRIL 18, 1984, pp. 3-4.


Special Committee on Youth Education for Citizenship,
