Invasion of Privacy: A 1984 Syndrome
by Dr. Suzanne H. Cook

During the summer of 1980, a grim story unfolded in Arizona. A young woman, who worked at an office supply store, refused to give her address to, or to date, a young man who kept coming to her workplace to see and talk to her. After getting her address from the state driver's license bureau, he went to her home and waited for her to return from work.

When she did, he shot her as she stood in the driveway.

At the moment of birth, hospitals gather information such as handprints, footprints, names, addresses, medical records, names of parents, names of brothers and sisters, and legitimacy data. For most people, schools become the next big gatherer of information with the accumulation of test scores, attendance, and behavioral and health records. Upon graduation, people begin to undergo further erosion of their privacy by releasing information to businesses through job applications, resumes, tests, and interviews. Businesses go a step or two—or three—further by requiring security checks through reference checking, secret monitoring devices, and visible monitoring devices. We should not be concerned about the information that is collected about them, but also about what information will be used, how it will be used, and who will use it. The key question becomes, "When does information-gathering become an invasion of privacy?"

A judicially approved definition of the right of privacy is "the right to be free from the unwarranted appropriation of one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities, in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities." The United States becomes more technologically oriented every day. Space satellites and computers add to information-gathering at a rapid speed. Technology has moved businesses into a level of monitoring and data-collection never before seen in the United States. This prolific gathering of information has individuals concerned. A Louis Harris poll showed that one-third of U.S. citizens believed this country could or would become much like fictional Oceania in George Orwell's 1984.

Should we be surprised at this perception? Current information-gathering discriminates against no one, and the information is disseminated without the individuals' knowledge.

Effects on Behavior

When there is an invasion of privacy, a person's physical and psychological safety can be affected, in turn affecting that person's behavior. One need only consider that the government has over four billion files related to everything from payrolls to social security data to criminal charges to loans and grants—most available at the touch of a button—to realize that privacy may be impossible. Voiceprints, spike mikes, microwaves, fingerprints, infrared cameras, electronic tracking devices, personality screening, lie detector tests, and behavioral profiles are only a few of the techniques used to gather information. Realizing that personal data may be obtained by anyone with access to a computer may lead to personality changes. The International Commission of Jurists in Geneva, in its 1972 study of the laws relating to the legal protection of the right of privacy, found that: "Some writers believe there is a danger of serious interference with the personal development of the individual resulting from the way in which he is 'presented' by the computer; in the last resort he may be driven to the point where he modifies his real personality to suit that presentation, behaving not in fact as he wishes but as he feels he is expected to behave 'objectively' and 'scientifically.'"

There is a further danger that the individual will become too conscious of his past rather than of his future. Such domination of the private life of the individual by technology could lead to a veritable pollution of the human personality.

With our society so tuned in to the use of machines, we may have begun to see individuals developing a blind faith in their accuracy. This blind faith will more than likely continue to grow as we move into the robot phase of technology and individuals begin to interact with robots. It is possible to influence with complicated technology, and this power can become overwhelming in the case of people who know nothing about the intricacies of how the machine works. Many people stand in awe of what they do not understand. Couple this awe with an authority figure, such as the administrator of the machine or the individual's manager, and our society has the capacity to influence great numbers of people. Since most people try to live up to the expectations of others, a definite self-fulfilling prophecy is possible. A pollution of the human personality could throw individuals and whole societies into a state of mental anquish. Mental and physical suffering is certainly possible when each year 250,000 to two million lie-detector tests are administered to Americans. One-fourth of all major corporations use the lie-detector tests.

The following cases, from William Petrocelli's Low Profile—How to Avoid the Privacy Invaders, show the effect of invasion of privacy one's physical and psychological safety.

- In one famous case, described in the book, Death in Canaan, an eighteen-year-old Connecticut boy was given a lie-detector test following the murder of his mother. After being told he failed the test, he gave a false confession to the police and was only acquitted years after a new trial.
- In Los Angeles, a food-store employee was asked "Did you check out items to your mother at a discount?" The

Dr. Suzanne H. Cook is an associate professor at Arizona State University as well as an active professor in the Center for Executive Development at ASU. She is listed in the World's Who's Who of Women, the Who's Who of American Women, and Who's Who in the West.
operator rated the employee’s response “deceptive,” and she was fired. Her emotional response, it turned out, was due to the fact that her mother was dead.

- Another case involved Linda Voikos, an employee of S. S. Kresge, a discount chain. Voikos reported $150 missing from the day’s receipts. After taking a polygraph test which she agreed to do, she was told she was the individual who stole the money and that she had deceived the company. Voikos, therefore, felt that she should quit before they fired her. After being traumatized by the event, Voikos spent two years in a varied stupor and fought off suicide. Six years later she began work in a doctor’s office where she is afraid to handle the bookkeeping. In 1979, a Detroit jury ruled against S. S. Kresge and ordered the chain to pay Voikos $100,000.

Not only does invasion of privacy affect physical and psychological safety, but invasion of privacy also affects an individual’s employment.

Effects on Employment

Invasion of privacy has long been a problem. In 1890, an article titled “The Right to Privacy” appeared in the Harvard Law Review. Since that time, technological advancements have increased the threat to individual privacy and have affected people’s employment opportunities. It is estimated that approximately nine million people seek initial employment or job advancement each year. This initial employment can be affected by invasion of privacy. To get a job in one-fourth of the major corporations in the United States, a person would have to be subjected to a polygraph test. A professional group at the Massachusetts Institute of Technology stated that this machine has an accuracy rate of approximately seventy percent; thus, one-third of the individuals taking the test could be denied employment based on an inaccurate machine reading. A polygraph, after all, measures not honesty but responses to tension and perspiration. The machine is not capable of probing into the innermost crevices of the mind. Thus, people who can control their emotions could possibly “lie to the lie detector.” And who is completely honest, but who cannot control emotions, can possibly be diagnosed as dishonest. Other errors can occur when an inexperienced operator is placed in charge of the machine. This low accuracy rate is alarming, but the abuse the prospective employee has to endure is even more alarming. During a polygraph test, potentially abusive questions relating to an individual’s sexual preferences, political views, and morality are intertwined with other psychologically probing questions. One definition of privacy is “the right of the individual to decide for himself...when and under what conditions his thoughts, speech, and acts should be revealed to others.”

With a polygraph test, the vitality of this concept is lost because the machine is designed to override the will of the individual and analyze involuntary physiological responses. Individuals experiencing this abuse have their privacy invaded and their job opportunities affected by questions that are not job-related. To maintain their job or to gain promotions, individuals have allowed invasion of privacy to grow. According to Petrocelli, an authority on invasion of privacy, “privacy is a luxury—far down the list of priorities that is headed by the need to earn a living wage.” This does not mean that people don’t care about their privacy, but it means that when their job hinges on their willingness to release information, they will give the information in order to “survive.” The ability of employees to protect their privacy may be nonexistent if they are dependent enough on one particular job,” Petrocelli adds. “A job defines a person’s station in life and puts bread on the table. The stark fact is that many people have no choice but to accept a job on any terms the employer wants to offer.” The implications of this “helplessness” is alarming.

“Wholesale invasions of privacy, says the United Nations, inhibit individual liberty,” according to the International Commission of Jurists. “The Community becomes fear-ridden, and no one can be trusted....This destruction of trust is one of the major dangers to a free society....The detailed questionnaire for employment, housing or insurance, the hidden or suspected camera, psychological tests, the lie detector—all these devices for ferreting out intimate details of our lives produce a pervasive insecurity which suppresses individuality, discourages responsibility and encourages frightened conformity.

Mrs. Sheck, a sought-after speaker and advanced applications system designer for Honeywell Inc., uses the following quote from the Arizona Republic’s Maggie Wilson in her speeches to illustrate that there is the potential for manipulation of employees if employers have access to “private” information about their employees:

“As every man goes through life, he fills in a number of forms for the record, each containing a number of questions. There are thus hundreds of little threads radiating from every man, millions of threads in all.

“If these threads were suddenly to become visible, the whole sky would look like a spider’s web. (But) they are not visible; they are not material, yet every man is constantly aware of their existence. Each man permanently aware of his invisible threads, naturally develops a respect for the people who manipulate the threads.”

As technology advances, will our society see “human puppets” dangling from threads afraid to speak or look sideways for fear of divulging their innermost thoughts which could cause more entanglement in the threads of manipulation? To have honest, private information manipulated is bad enough, but it is tragic when false information is manipulated affecting an individual’s life. False information was used in the following case, described by the late Earl Warren:

“A talented young lady was unable to gain employment for some time following graduation from college because potential employers were wary of an entry in her university file that she became aware of only after many painful experiences. It said, “Melinda’s mother is emotionally unstable.” It turned out that this comment had been made by the girl’s sixth grade teacher, who was neither a psychiatrist nor a psychologist and had only met the child’s mother casually. Yet this damaging entry had been preserved and had followed Melinda for 15 years without anyone questioning either the propriety of its retention or its reliability or relevance.

There are many “Melindas” in our society who are anxiously looking for jobs and are being adversely affected by erroneous information stored in some businesses’ files. An initial job offer, job retention, and job advancement can hinge upon information that should never have been acquired and retained by employers. Thus, people are becoming protective of their private information.

Those who realize how information about them can be manipulated to their detriment are becoming reluctant to communicate in writing or verbally and are attempting to gain control of information accumulated about them. Robert Smith, author of Privacy: How to Protect What’s Left of It, suggests that, “If printed forms ask information you consider private, you can always write ‘Irrelevant’ for ‘irrel-
Invasion of Privacy

has been asked by representatives of organized labor to approve legislation banning the use of polygraphs in the workplace (H.R. 1524, 1924).

Specific Recommendations
1) Collect information only if the need has been established in advance.
2) Collect information, when possible, directly from the subject. Avoid fraudulent or unfair means of collecting data.
3) Verify with the subject involved if information is correct. Incorrect data or discriminatory data should be purged from the files.
4) Allow subjects to review their files, correct, erase, or amend inaccurate, obsolete, or irrelevant information. Accept an individual’s statement of dispute, and allow statement of dispute to be accessed and transferred with other related data.
5) Secure the information system from any reasonably foreseeable threats to its security.
6) Do not maintain secret files on individuals. Allow subjects to find out what information is stored on them, the purpose for which it is collected, and how it is to be used or disseminated.
7) Maintain records of organizations or employees having regular access to personal information on a “need to know” basis, and of the nature, date, and purpose of access to that information, by them and others.
8) Release to third parties (outside parties) only “directory information” such as position and dates of employment unless the employee gives written consent to the release of additional data, a judicial order, or a subpoena. Obtain verification that the third party is a properly identified individual who has a legitimate right to the information.
9) Gain assurance that information released will be used only for the purposes set forth prior to the release of the information.
10) Store information regarding access to information for five years, or the life of the record, whichever is longer.

References

Recommendations to Help Safeguard Privacy

The following recommendations, both general and specific, should be considered to help safeguard employees’ privacy and to help ease the liability that can be incurred by the employer who invades employees’ privacy.

General Recommendations
1) Become familiar with the Privacy Act of 1984 which covers the public sector.
2) Become proactive and setup guidelines to protect information in your organizations.
3) Monitor legislation currently under consideration. The House Labor Subcommittee on Employment Opportunities

20/1M, September-October 1986