IEEE Spectrum's zeal in reporting on cutting-edge technologies and trends has at times led to insights whose importance extends well beyond the traditional borders of electrotechnology.

Consider an article by Charles P. Lickson, a corporate counsel for a small company who had also clerked in the Federal judiciary.

In his 'Privacy and the computer age' (October 1968, pp. 58–63), Lickson looked at the growing use and sophistication of electronic devices and found it a threat to individual and corporate privacy rights. His thoughts remain relevant to this day, with the issue of privacy versus telecommunications a more hotly debated topic than ever.

The concern for privacy—a right perhaps remembered more in breach than in observance in the United States—looms large when consumers pick up on new modes of communication like the Internet and cellular telephony. Lickson reminded his readers that privacy is not a constitutionally protected right. He began by noting that “[i]n the year 2000, Americans could have computers and robots in the home—and virtually no privacy,” and listed a number of intrusions into individuals’ privacy that were already taking place.

“Investigators keep tabs on their victims through sophisticated technological means…Phones are tapped. Rooms are bugged. Employment interviews seek the most personal information. Data on all aspects of individual and corporate existence are being centralized in huge data banks. Computers are being shared. Government is increasing in its size and centralization of activities.”

When the article was written, only 21 states allowed an individual or corporation to sue another for damages arising out of invasion of privacy. Two more recognized the right, but limited it by statute. The failure of every state to have such a policy was due to the lack of a clear definition of what should be considered private. But Lickson observed that traditional definitions of what was private, according to state laws and judicial opinions, had already been rendered obsolete by advances in technology like electronic sensors and listening and monitoring devices.

Lickson noted that law enforcement agencies and other government entities could with impunity listen in on remote conversations and monitor remote movement because neither activity fell within the bounds of search and seizure rulings handed down by U.S. Federal courts. In Lickson’s view, congressional action was needed to establish policies governing scientific and technological matters. He argued that technological advancement had paved the way for a dramatic alteration of the U.S. Federal system that “has made Congress, and not the Supreme Court, the final arbiter in government.”

The Supreme Court recognized the duty to protect people against invasions into “constitutionally protected areas,” but laws enumerating what was protected had yet to be written by Congress, report-
ed Lickson. Important statutes such as the Privacy Act of 1974, the Right of Financial Privacy Act of 1978, and the Electronic Communications Act of 1986, which today provide protection against intrusion (or at least provide a means for legal redress), were years in the future.

To regulate the government’s use of technology to invade individual privacy, Lickson described three possible approaches that would apply to corporations as well as to individuals. The first sought to eliminate pooled data centers and intelligence systems by drafting legislation that would outlaw or tightly restrict such activity. Lickson noted that this view stemmed from a belief that privacy could not be sacrificed for improved technology, but felt it was too extreme. Imagine the effect this would have on the way business is done today. Records of personal information are kept almost everywhere. Hospitals, health maintenance organizations, insurance companies, mortgage lenders, the Internal Revenue Service—indeed, just about every company imaginable—maintain databases containing personal information about their clients and employees. Lickson felt that a frenzied, though well-meaning attempt to prevent further erosion of the right of privacy could threaten relatively benign and clearly beneficial caches of data.

The second approach to regulating the use of technology, according to Lickson, would maintain the current state of affairs. The assumption here was that the safeguards then in place were sufficient and that industry and government would police themselves.

The third approach, which Lickson himself espoused, presumed that new legal protections would be necessary to prevent erosion of the individual’s right of privacy. Lickson stated that as long as technology continues to expand the ways in which human beings can interact with it and with each other, new laws must address these changes.

Lickson was correct in predicting that the states that had refused to recognize the right of privacy would soon do so. Today, every state has a statute, short or detailed, related to privacy in data communications and/or computer crimes such as hacking. Also accurate was his view of the future role of private industry.

“…until legislation and court decisions can catch up to the state of the art—much of the burden of providing security for data and assuring privacy rests with private industry.”

Today, obtaining any of a host of goods and services like borrowing money, making major purchases, or getting medical treatment requires one to first answer a litany of personal questions—few of which are optional. Thus far, companies have used their data-gathering resources primarily for marketing purposes. Selling lists containing the names and addresses of people who have used a particular product or service, or who have a particular organizational affiliation is a common practice. An example is a person who has a second home phone line installed and soon receives unsolicited mail from long-distance carriers.

The government has yet to weigh in with restrictions on the selling of mailing lists, nor has it determined once and for all whether information voluntarily given to a company for business purposes ceases to be private. This has left the future of privacy in the hands of private industry—entities that, true to their intrinsic nature, place profit above all other concerns.

WILLIE JONES, Editor

IEEE SPECTRUM OCTOBER 1998