# Chapter 1
# Summary

# Chapter 1

# Summary

In the last 20 years, there has been a virtual revolution in the technology relevant to electronic surveillance. Advances in electronics, semiconductors, computers, imaging, data bases, and related technologies have greatly increased the technical options for surveillance activities. Closed circuit television, electronic beepers and sensors, and advanced pen registers are being used to monitor many aspects of individual behavior. Additionally, new electronic technologies in use by individuals, such as cordless phones, electronic mail, and pagers, can be easily monitored for investigative, competitive, or personal reasons.

The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance applications. The fourth amendment–which protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures' '—was written at a time when people conducted their affairs in a simple, direct, and personalized fashion. Telephones, credit cards, computers, and cameras did not exist. Although the principle of the fourth amendment is timeless, its application has not kept abreast of current technologies.

The major public law addressing electronic surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which was designed to protect the privacy of wire and oral communications. At the time Congress passed this act, electronic surveillance was limited primarily to simple telephone taps and concealed microphones (bugs). Since then, the basic communications infrastructure in the United States has been in rapid technological change. For example, satellite communication systems and digital switching and transmission technology are becoming pervasive, along with other easily intercepted technical applications such as cellular mobile radio, cordless telephones, electronic mail, computer conferencing, and electronic bulletin boards. Continued advances in computer-communications technology such as the Integrated Services Digital Network (ISDN), now close to implementation, are likely to present additional new opportunities for electronic surveillance.[1]

The law has not kept pace with these technological changes. The courts have, on several occasions, asked Congress to give guidance. Most recently, U.S. Circuit Court Judge Richard Posner, in a case involving the use of video surveillance in a law enforcement investigation, said:

> . . . we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope . . . judges are not authorized to amend statutes even to bring them up to date.

In legislating the appropriate uses of electronic surveillance, Congress attempts to strike a balance between civil liberties—especially those embodied in the first, fourth, and fifth amendments to the U.S. Constitution–and the needs of domestic law enforcement and investigative authorities for electronic surveillance in fighting crime, particularly white-collar and organized crime, and generally for drug, gambling, and racketeering investigations.'

Law enforcement and investigative agencies, at least at the Federal level, are making significant use of electronic surveillance techniques and are planning to use many new techniques. Based on a review of available reports

[1]ISDN permits the transmission of voice, video, and data signals as needed over a common multi-purpose communications network,

[2]Note: This study did not review technology or policy issues concerning foreign intelligence and counterintelligence applications of electronic surveillance.

and the results of its Federal Agency Data Request,[3] OTA found that:

- The number of Federal court-approved bugs and wiretaps in 1984 was the highest ever.
- About 25 percent of Federal agency components responding (35 out of 142) indicated some current and/or planned use of various electronic surveillance technologies, including, but not limited to, the following:
  —closed circuit television (29 agencies);
  —night vision systems (22);
  —miniature transmitters (21);
  —electronic beepers and sensors (15);
  —telephone taps, recorders, and pen registers (14);
  —computer usage monitoring (6);
  —electronic mail monitoring or interception (6);
  —cellular radio interception (5);
  –pattern recognition systems (4); and
  —satellite interception (4).
- About 25 percent of Federal agency components responding (36 out of 142) report use of computerized record systems for law enforcement, investigative, or intelligence purposes:
  —agencies reported a total of 85 computerized systems with, collectively, about 288 million records on 114 million persons;[4]
  —examples of four such systems that could be used in part for data base surveillance purposes are the:
    1. National Crime Information Center (FBI),
    2. Treasury Enforcement Communications System (Treasury),
    3. Anti-Smuggling Information System (Immigration and Naturalization Service–INS), and
    4. National Automated Immigration Lookout System (INS).
  —none of the 85 system operators provided the requested statistics on record quality (completeness and accuracy). Most do not maintain such statistics.

After conducting a review of the technology and policy history of electronic surveillance, OTA found that:

- The contents of phone conversations that are transmitted in digital form or calls made on cellular or cordless phones are not clearly protected by existing statutes.
- Data communications between computers and digital transmission of video and graphic images are not protected by existing statutes.
- There are several stages at which the contents of electronic mail messages could be intercepted: 1) at the terminal or in the electronic files of the sender, 2) while being communicated, 3) in the electronic mailbox of the receiver, 4) when printed into hardcopy, and 5) when retained in the files of the electronic mail company or provider for administrative purposes. Existing law offers little or no protection at most of these stages.
- Legislated policy on electronic physical surveillance (e.g., pagers and beepers) and electronic visual surveillance (e.g., closed circuit TV and concealed cameras) is ambiguous or nonexistent.
- Legislated policy on data base surveillance (e.g., monitoring of transactions on computerized record systems and data communication linkages) is unclear.
- There is no immediate technological answer to protection against most electronic surveillance, although there are emerging techniques to protect communication systems from misuse or eavesdropping (e.g., low-cost data encryption).[5]

OTA identified a range of policy options for congressional consideration:

- Congress could do nothing and leave policymaking up to the development of case

[3]The data request was sent to all major components within the 13 cabinet-level agencies and to 20 selected independent agencies. Due to the unclassified focus of this study, two Department of Defense components–the National Security Agency and Defense Intelligence Agency–along with the Central Intelligence Agency were excluded from the data request.

[4]Extent of multiple records on the same person is unknown.

[5]Technical options are being addressed in a separate OTA study on "New Communications Technology: Implications for Privacy and Security," expected to be published in winter 1986/87.

law and administrative discretion. However, this would lead to continued uncertainty and confusion regarding the privacy accorded phone calls, electronic mail, data communication, and the like, and ignores judicial requests for clarification in areas such as electronic visual surveillance.

- Congress could bring new electronic technologies and services clearly within the purview of Title III of the Omnibus Crime Control and Safe Streets Act, for example by:
  - –treating all telephone calls similarly with respect to the extent of protection against unauthorized interception, whether analog or digital, cellular or cordless, radio or wire;
  - –legislating statutory protections against unauthorized interception of data communication;
  - –legislating a level of protection across all stages of the electronic mail process so that electronic mail is afforded the same degree of protection as is presently provided for conventional first class mail;
  - —subjecting electronic visual surveillance to a standard of protection similar to or even higher than that which currently exists under Title 111 for bugging and wiretapping.
- Congress also could set up new mechanisms for control and oversight of Federal data base surveillance, for example by:
  - —requiring congressional approval of specific Federal data base surveillance applications (e.g., by statutory amendment or approval of House and Senate authorizing committees);
  - —establishing a data protection board to administer and oversee general statutory standards for creating and using data bases for purposes of surveillance.
- Congress also could amend the Computer Fraud and Abuse Act of 1984 to cover interstate computer crime.
  - —This option, not detailed here, could provide additional legal protection against unauthorized penetration (whether for surveillance or other reasons, e.g., theft or fraud) of computer systems.[G]

Chapters 2 through 5 of this report provide technical and policy analyses relevant to proposed legislation on electronic surveillance and civil liberties, such as the "Electronic Communications Privacy Act of 1985' and the "Video Surveillance Act of 1985.'"

[G]See the computer crime chapter of the forthcoming OTA report on "Federal Government Information Technology: Key Trends and Policy Issues" for discussion.

'H.R. 3378 introduced by Rep. Robert Kastenmeier and S. 1667 introduced by Sen. Patrick Leahy. See U.S. Congress, House of Representatives, *Congressional Record,* Extension of Remarks, Sept. 19, 1985, p. E-4 128; and U.S. Congress, Senate, *Congressional Record,* Sept. 19, 1985, p. S-11 795.

'11. R. 3455 introduced by Representative Kastenmeier. See U.S. Congress, House of Representatives, *Congressional Record,* Extension of Remarks, Sept. 30, 1985, p. I+; -4269.