INTERACTIVE HOME MEDIA AND PRIVACY

Prepared for
OFFICE OF POLICY PLANNING
FEDERAL TRADE COMMISSION
by

Deanna Collingwood Nash, Ph.D.
John B. Smith, Ph.D.
COLLINGWOOD ASSOCIATES, INC.
2025 I Street, N.W., Suite 519
Washington, D.C. 20006
with
Susanna Bolten
Nancy Stiff

JANUARY 1981

TABLE OF CONTENTS

Interactive Home Media and Privacy Issues

INTERACTIVE HOME MEDIA AND PRIVACY ISSUES

I. Purpose of the Report

A. Framework for the Report

The Federal Trade Commission, Office of Policy Planning, wishes to explore the consumer-related privacy issues associated with the new interactive home media developing or currently operating in the U.S. Its initial goal is to identify the role, if any, the FTC should play over the next several years to meet its congressional mandates. To accomplish this goal, the FTC must understand the general nature of the privacy issues associated with interactive home media. It has contracted with Collingwood Associates, a Washington-based consulting firm specializing in telecommunications, to provide an initial analysis of the issues and to set a framework for further study (Contract #L0678). To accomplish this task, Collingwood Associates has highlighted the technical aspects of three types of interactive home media and outlined some of the consumer-related privacy issues arising out of their design, management, and use. (See Appendix I., Background.)

B. What This Report Does and Does Not Do

This report provides basic information about three types of interactive home media: interactive cable systems, interactive videotex-teletext systems, and general purpose computer systems. Within each type or "model", it identifies one or more examples--systems that are operating in the U.S. today or are being formally tested in the U.S., having been

developed and operated first in other countries. Within the description of each model and primary example, this report highlights those system points where privacy issues do (or might) arise. It sets this information in a broader context--that of the prevailing concepts of privacy, both legal and social.

The report is based on both primary and secondary sources. Key personnel in the interactive home media companies (cited as examples for each model) were interviewed by Collingwood Associates on-site. Many secondary sources were reviewed, including law review articles; telecommunications reports; and privacy studies by academics, non-profit groups, trade associations, corporate entities, and others.

This report does not list all privacy questions associated with interactive home media. Nor does it describe all possible models of these systems. Also, it does not relate all legal discussions of privacy to these systems.

Instead, it is organized to provide a general framework for considering questions of privacy in this arena--interactive home media--and for determining the research steps necessary for understanding the best ways to protect consumers' privacy in the years to come. Until these next steps are taken, goals and strategies for handling privacy issues cannot be selected by federal agencies and others.

C. Next Steps

The next research steps required are:

- to complete a full-scale examination of federal, state, and local statutes pertaining to privacy;

- to study the economic structure of the interactive home media industry as it bears on privacy and other consumer concerns;
- to organize these legal and economic concepts in a manageable framework;
- to survey all federal agencies for their current activities specifically touching upon the question of privacy and to determine how existing activities relate to interactive home media; and
- to develop an inter-governmental plan to develop strategies for action, where governmental action is warranted.

In short, the report that follows will serve those currently unfamiliar with the developments in the interactive home media field to begin to explore the possible areas of concern about privacy. Further research, particularly legal research, as well as extended discussions with entrepreneurs in the interactive home media industry and with consumers of these services will be necessary next steps before the Federal Trade Commission can define its role in this arena.

II. Privacy

A. Definitions

The current status of the concept of privacy is far more complicated than it appears at first glance. We have examined many secondary sources (see Appendix V., Bibliography) to get a sense of the state of privacy as a concept in the U.S. today. What we have discovered is that privacy, as a legal concept, is still in a state of flux. No one seems to disagree that there is some kind of individual right of privacy. But from there on, there is little agreement on the nature--definitions or limits--of that right.

Cases have established several privacy doctrines, such as:

- the need for consent to use a person's likeness "for advertising purposes or purposes of trade" (1903 N.Y. Laws chs. 113 §§ 1,2; presently N.Y. Civ. Rights Law §§ 50-51, McKinney 1948);
- the right of individuals to know what information exists in a data bank about them and the right to have errors corrected (applying to federal data bases, The Privacy Act of 1974); and
- the need to restrict the aggregation of data by consolidation of data bases or the exchange of data among data bases, since data that might be innocuous when viewed separately may be embarrassing or injurious to the individual when aggregated (applying to federal data bases, The Privacy Act of 1974).

In all, though, these cases are not yet a means to understanding the concept of privacy--not until a formal framework is designed to summarize the doctrines established so far can we begin to create the zones of protection the FTC should seek to develop. Two recent law review articles attempt to develop a kind of framework, at least to array the various legal definitions of privacy and to place them in some larger, social context.[1] In addition to the need to develop a framework of privacy doctrine is the need to relate the legal doctrines established in certain types of cases (those dealing with privacy issues raised by the computerization of criminal, health, banking, and other personal records) to the interactive home media systems. Perhaps when such research is completed, it will show that the privacy issues in these cases are basically

---

[1]For examinations of the prevailing variety of definitions of privacy, see: R. Gavison, Privacy and the Limits of Law, 89 Yale L. J. (January 1980); and T. Gerety, Redefining Privacy, 12(2) Harv. C.R.L. L. Rev. (Spring 1977).

no different from the ones associated in this report with interactive home media systems. In such an event, of course, the bulk of our work will have been done.

At any rate, to define what privacy is, one must turn not only to legal but to social definitions, definitions based on how individuals seem to function in society.[2] Individually, we all seem to have a sense of privacy--of maintaining control of information about ourselves, of sharing as we see fit, of having what we share be used as we intended.

Ultimately, then, the current concept of privacy seems to be widespread and ingrained at the same time as it is not easily definable or protectable. The whole concept really seems to require a philosophical (legal and other) analysis.

See Appendix II. for more details on the status of the privacy concept.

B. Common Elements

When consumers use the interactive home media systems--whether by retrieving information, answering inquiries, ordering goods and services, or using security and other monitoring services--they are conveying to a central computer at the "head-end" information about themselves: their interests, choices, views, and more. How is their privacy protected at this time?

---

[2] See works by A. Westin, including Privacy and Freedom (1967). Westin's approach to defining privacy is highlighted in Appendix II. of this report.

In its detailed analysis of three models of interactive home media (see Appendix III.), this report indicates points where consumers might be risking their privacy. We have especially focused on four major types of exposure:

- intrusion;
- interception;
- misuse of information; and
- aggregation by household.

Future research, particularly the development of a framework for privacy, will help refine these categories.

1. Intrusion

The interactive home media offer several monitoring services: home security devices to detect smoke, fire, sound, movement; energy load management; and medical. Some of these services protect consumers from forms of intrusion (such as theft) or other privacy infringements. But they also have the potential, if not carefully circumscribed, of being forms of intrusion themselves. If companies shared any monitoring information with others (other than to call fire trucks or ambulances as needed by the emergency signal received), the issue of intrusion is raised. For example, a utility company, noting consumers' uses of the energy load management system, might use that information not simply to regulate the household's heat, as requested in the monitoring service, but go on to develop energy policies to affect that household.

Another form of intrusion is the undesired reception of objectionable, obscene, offensive, or unwanted programs (or

"frames" or computer-supplied information). This privacy issue is raised in some interactive home media systems (see Section III. below). But it is not peculiar to these media; it obviously occurs in over-the-air broadcasting, in one-way cable systems, and so forth.

2. Interception

Interception is eavesdropping on--or unauthorized access to--a private communication by the consumer to the head-end computer. Interception can happen at several points in an interactive system:

- in the transmission of the communication between the home console or TV and the head-end computer; and
- at the head-end, either by an undesignated employee accessing data or by forced access by a source outside the interactive media system.

This kind of privacy issue appears to be the same as the confidentiality problem faced in the computer industry by computer room operators and other personnel. Safeguards found to be sufficiently effective for secure and classified systems may prove useful, even adequate, in this interactive home media arena: if they are faithfully and formally used.

3. Misuse of Information

Consumers likely provide information through an interactive system on the basis:

- that they will not be identified as individuals but rather that the information they provide will be added to a group's tally; and
- that the information will be used as they intend it and no way else.

Consumers may purchase goods and services through their interactive home media system. They expect to receive those items and to be billed for them. (If they pay by credit card, they likely expect that their credit information is used only to handle the transaction itself.) But they do not expect to have information about their purchases circulated to other businesses or entities. Consumers watch programs or "frames" and expect to be billed for them. They do not expect to have information on their viewing selections and habits released--on a by-individual or by-household basis--to others. Such a release of information would raise the privacy issues of the misuse of information. Aggregation of the information, where each individual is not--and cannot--be identified, does not seem to raise a major privacy issue. At the least, consent of the individual or household should be obtained before any information about them is released on an identifiable basis.

Another aspect of this privacy issue is the individual's right to know what information exists in data banks about them and to have errors corrected. (So far, this kind of right is protected in federally maintained data bases.) Further, consumers need to be educated about the privacy implications of the interactive services.

4. Aggregation by Household

A major exposure of privacy exists in the aggregation of individually insignificant or innocuous data to form a characterization of a person, household, or group. Viewers' program choices, product or service purchases, financial

information, or other information available through their use of an interactive home media system might be aggregated in a way to embarrass, damage, or otherwise affect their privacy. Patterns discerned from this information could be used to form "psychographic" profiles of a household--profiles that could be used to devise marketing strategies to which members of the household would be particularly vulnerable. In addition, aggregated information about an individual or community could be transferred to a parent corporation, possibly giving unfair competitive advantage in a different and unrelated area of activity. These, we believe, are privacy issues.

5. Other Issues

Beyond the four major privacy issues listed above, there are a few miscellaneous, but important privacy issues centering around these kinds of questions. What do the above-named kinds of risks mean to consumers of the interactive home media services? Do consumers know about these risks when they purchase interactive services? Do the services they purchase change in nature, without their knowledge?

Interactive media services, while not extensive at this time, are expected to grow significantly over the next few years. We looked at some of those now operating to learn which of these privacy issues might have been raised already.

III. Three Models of Interactive Home Media

This report looks at three types of interactive home media:

- Interactive cable systems;
- Videotex-teletext systems; and
- General purpose computer systems.

Within each type, a major example is selected to focus the study.

Details on all three systems are found in Appendix III.

A. Brief Description of the Models

1. Interactive Cable Systems

Interactive cable systems are an outgrowth of the conventional one-way cable delivery system for television. Instead of transmitting a signal only "downstream" from the signal source to the viewer, they are able to transmit some form of signal originating at or near the receiver back "upstream" to the head-end where it is usually received by a monitoring computer. The specific example of this model described in this report is the Warner-Amex Qube system operating in Columbus, Ohio. (See details on this system in Appendix III. A.)

In our study of this one interactive cable system, we did not identify any breaches of privacy--only the potential for such breaches. The Qube system design and management have safeguards to protect privacy, but these have not been codified (as far as we can ascertain) into an actual, comprehensive written policy. The Qube system managers do see the protection of privacy as in their self-interest, since virtually all revenues are derived from consumers at this time. Of note,

Qube was subpoenaed for records on their "adult" channel viewing selections by individual rather than aggregate. Qube released that information only on the aggregate basis, thereby protecting the privacy of their individual subscribers (but not the subscribers as a group). The potential of Qube's sharing information about individuals with its parent corporation, American Express, is there and raises the privacy issue of aggregation by household.

2. Videotex-Teletext Systems

Videotex and teletext systems offer the user formatted pages of information displayed on a TV set using a conversion unit, installed separately or incorporated in some of the newer specially designed TV receivers. The interactive versions are examined in this report. These are in various testing stages in the U.S., having been designed elsewhere. Three consumer-oriented systems serve as examples of this model: Prestel (British), Telidon (Canadian), and Antiope (French). (See details in Appendix III. B.)

The potential for the infringement of privacy may be even higher, at this time, in such systems than in the interactive cable systems. These systems accept information provided by all who wish to pay to have their information entered into the system. There is no single point in the system now held accountable for the misuse of information or the aggregation of information. Unlike interactive cable systems (where a single corporation controls the head-end computer(s), the transmission system, the receiver, and to a

large extent, the programming content), videotex-teletext systems represent abutments of a number of different independent corporations. No one deals comprehensively with the entire system. Since issues of privacy often emerge at the interfaces of information transfer subsystems, the alignment of financial interests and separate policy spheres at precisely those points of contact is likely to leave unclear where, exactly, responsibility for privacy lies. It is important to note, however, that for the Prestel system, there is a trade association of all organizations, private and public, participating in that system; they have agreed upon a "Code of Practice": to exercise some control on this system, at least at the level of the "frames" made available to consumers. As to the question of privacy, this code speaks to unauthorized access only; and it does not focus on points of "interface" throughout the system.

Otherwise, these examples of interactive videotex-teletext systems share with the other types of interactive home media the privacy issues of intrusion and interception. And as with the others, it is difficult for consumers to ever learn that their privacy has been breached. Again, consumers may not even know about the privacy implications of the services in the first place.

3. General Purpose Computer Systems

The third type of interactive home media is the system offering general computer retrieval and other services to the consumer. This type of system employs standard data processing

links and standard computer terminals, rather than converted TV sets, as output devices. As a result, the nature and form of the information provided the user are different from that provided by the other systems described in this report. Information is not necessarily page-oriented, although some specific requests are printed or displayed in a page format; rather, information is more likely to be displayed as a continuous succession of lines. Information is primarily textual and character-oriented; no graphic output is currently provided. However, a much larger range of interaction is possible. The specific example of this model described in this report is The Source. (See details in Appendix III. C.)

This type of interactive home media shares with the others the potential for the infringement of privacy along the four categories of privacy outlined above. Consumers' communications--their personal financial data, messages, and other information maintained in the general purpose computer system--are protected by passwords. However, the misuse of information and the aggregation of information are potentially privacy issues--if company staff, consultants, or unauthorized persons use those passwords to gain access to information to which the consumer has not consented release or use. Such a privacy issue is common to the computer industry and is not therefore peculiar to the interactive home media industry itself. Consumers of the service, however, need to know this similarity as they purchase the service; and they need safeguards, including written agreement from the company from whom they purchase the

service that their privacy will be protected. (Future research will highlight stronger measures, if warranted, than such agreements suggested here.)

B. Common Elements

The interactive home media field is new and burgeoning. As a group or as individual companies, the interactive service providers have taken few formal steps to write their policies on privacy, to issue guidelines to their staff to protect the consumers' privacy, or to inform their subscribers about the potential risks to their privacy. Even if consumers had such information, they could do little as individuals to protect their privacy. They depend now, and likely in the near future, on the companies from whom they purchase the services to protect their privacy. These companies, dependent to a significant degree on consumer financing, wish to protect their consumers' privacy interests--but in some kind of cost-efficient way. They may even have plans at this moment to write their privacy policies and procedures and distribute them. However, the fact of the matter is that much more can--and needs to--be done with regard to protecting consumers' privacy in these new interactive home media systems.

IV. Next Steps--Recommendations

We are not in a position--having completed this first step toward fully exploring the privacy issues associated with interactive home media--to recommend how each model, or example of a model, should handle each privacy issue identified. Rather,

we have developed recommendations pointing out where the research should go from here. Our recommendations fall into these three categories:

- Further refining protectable privacy interests;
- Developing strategies for protecting consumer privacy (including the privacy of businesses as consumers of these services); and
- Handling other privacy issues.

A. Refine Protectable Interests

Before the Federal Trade Commission, other federal agencies, or others involved in protecting the consumers take action in the area of interactive home media and privacy, they will need to refine what the protectable privacy interests are. A framework for these interests needs to be developed. As our selected bibliography (Appendix V.) indicates, there has been considerable discussion of all facets of the concept of privacy in both its legal and social definitions. (A good deal more work, we believe, could be applied to the underlying philosophy of each.) These works, however, approach just one or two aspects of the concept at a time. And a framework for policy makers--whether at the businesses operating these systems or in governmental agencies--has not been developed. We recommend that a study be undertaken to develop such a framework. The Federal Trade Commission alone or in coordination with others could undertake or commission such a work.

B. Develop Strategies

A major set of strategies needs to be developed to deal with the privacy issues associated with the interactive home media over the next few years. This set of strategies would fall into three categories:

- General regulations;
- Self-regulations; and
- Consumer education.

1. General Regulations

There needs to be an examination of the information resulting from the legal search and framework recommended above in order to understand what kind of strategies to protect privacy can be derived from existing statutes and what strategies require new statutes and subsequent administrative regulations.

2. Self-Regulations

The companies in the interactive home media business are capable of, and may wish to, establish standards for protecting consumer privacy for their corporate entities. They can also work together to develop industry-wide standards in this area. We recommend that these standards be developed formally, that they be written policies and procedures for protecting privacy. We further recommend that they be part of the contracts between consumers and service providers and that consumers be notified of changes in the services as they occur.

3. Consumer Education

A key to this whole subject is letting consumers know what their purchase of interactive home media services involves, particularly what risks to their privacy they may be running under current law and practice. The relationship between the services and a consumer's privacy is not foremost on a consumer's mind; they may not even know the technology well enough to know about the risks at all. We recommend that the appropriate federal agencies and the interactive home media service providers begin now to educate consumers about what the interactive home media systems entail and how they might affect privacy. However, this activity cannot replace the steps suggested above.

C. Other Steps

We recommend that any analysis exploring ways to regulate the interactive home media for the protection of privacy examine the industry, and each system in it as a whole. In the long run, regulations may be addressed to particular segments; but these must first be based on the further identification of privacy concerns as they extend throughout each system. Only in this way can domains of responsibility be fixed. Only by looking at the system as a whole can one see clearly consumer interests and assign responsibility, especially in those cases where more than one vendor now shares responsibility.

D. What the Federal Trade Commission Should Do

We recommend that the Federal Trade Commission take the following six steps as quickly as possible:

1. Undertake or commission a full-scale examination of federal, state, and local statutes pertaining to privacy that do or can relate to the interactive home media field. This study should include a survey of all federal agencies for their current activities and plans specifically touching upon the question of privacy. The product of such a study should include a framework of privacy interests for policy makers.

2. Undertake or commission a study of the economic structure of the interactive home media industry, especially as it bears on privacy and other consumer-related concerns.

3. Determine the level of privacy protection needed and feasible.

4. Encourage forms of industry self-regulation in this area.

5. Provide consumer education services, including printed material, about these new media.

6. Work on an inter-governmental plan to develop strategies for action, where government action is warranted.

* * *

The question posed by the Federal Trade Commission is vital to all of us: What is the status of privacy in the interactive home media industry today? It is a complicated question. The interactive home media industry is a fast-growing

sector of our economy, part of the oft-called Information Industry considered to be one of the largest sectors of the economy. The question of privacy in this field should be foremost on the minds of the company managers offering these services, the government policy makers who regulate aspects of these or related services, and citizens, all of whom have the right to privacy (however it can be defined) under the Constitution. We cannot urge strongly enough that the research steps we have suggested--as well as steps others offer--should be taken as soon as possible. When the interactive home media industry is a little older and more established, it will be more costly and difficult to require designs and management that protect privacy. Exploring the question early will allow that design and management to be built into the systems as they develop, and crises of breaches of privacy can be minimized.

Appendix I.

BACKGROUND

Appendix I. BACKGROUND

Interactive home media are those electronic communications systems that use computer technology to provide services to customers--to varying degrees--in response to directions or inquiries.

Services that are offered by these systems (or anticipated in the near future) include:

- publication services - wire services including news, financial, sports, and congressional information.
- financial services - market reports, routine accounting services, and electronic funds transfer.
- shopping services - mail order merchandising, a wide variety of ticket and reservation services, and comparative shopping information.
- message services - electronic mail, a variety of transactional services, word processing and text formatting.
- entertainment services - schedules of events and games.
- educational services - instructional material and drills.
- monitoring services - home security devices to detect smoke, fire, sound, movement; energy load management; medical oversight.

Proponents of the interactive home media offering (or planning to offer) these services note their consumer benefits: greater choice, access, transportation and time savings, safety, and more. Underlying all these potential benefits, however, is one major concern: in what ways do consumers

subscribing to these services risk their privacy? After all, when consumers retrieve information, answer inquiries, order goods and services, or use the security and other monitoring services of these systems, they are conveying to a central computer at the "head-end" information about themselves: their interests, choices, views, and more. How is their privacy protected at this time?

This report and the remaining appendixes examine this question and establish a general framework for understanding the privacy issues raised by these systems.

Appendix II.

PRIVACY

Appendix II. PRIVACY

Before focusing on three types of interactive home media--and the privacy issues raised by these new technologies--let us take a look at what "privacy" means. A discussion of privacy would best begin with some kind of standard definition of the term or, at the very least, with a few of the most widely accepted definitions. But there is as yet no standard, legal definition or even a widely accepted framework of definitions.

Four definitions, covering the years 1890-1980, indicate some of the range in concepts of privacy:

> ...to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Warren & Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
>
> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. A. Westin, Privacy and Freedom (1967).
>
> Privacy is the control over or the autonomy of the intimacies of personal identity. T. Gerety, Redefining Privacy, 12(2) Harv. C.R.L. L. Rev. (Spring 1977).
>
> Privacy is a limitation of others' access to an individual... A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him. R. Gavison, Privacy and the Limits of Law, 89 Yale L. J. (January 1980).

Above, Westin claims absolute control over all information about the self for groups as well as individuals; Gerety, on the other hand, in an attempt to carve our functional distinctions that can limit as well as include, restricts privacy to issues of "intimacy", particularly those of a physical sort. Perhaps the ultimate definitional dilemma is found in the "reductionist" position that actionable infringements never are for invasion

of privacy, per se, but for other losses that are suffered coincidentally. (See R. Gavison, Privacy and the Limits of Law, 89 Yale L. J., January 1980, for a full discussion of the "reductionist" position.)

These four definitions, and many others not mentioned here (see Appendix V., Bibliography, for references), differ in subtle but profound ways. The issues of difference are quite complex in their legal and social ramifications. We, of course, cannot presume to enter this discussion in a report of this nature. Instead, we will briefly outline the legal foundation in this country for the concept and protection of privacy. Next, we will highlight the social and cultural concepts of privacy. While protection of privacy must rest ultimately on the legal system, it is clear (a) that the concept of privacy is much broader and deeper in the minds, social patterns, and expectations of the citizenry than in codified or case law; and (b) that new communication and data handling technologies raise questions not yet fully or adequately addressed within the legal system. Last, we will outline several major areas of concern about privacy that will likely emerge in connection with the fast-growing consumer information industry.

A. Some Legal Definitions of Privacy

While the Constitution does not address the issue directly, privacy as a concept is both a part of the general intellectual framework in which it is cast and an underlying value on which a number of protections rest. The influence of Locke's

thought on the authors of the Constitution is well known. As Alan Westin has observed, Locke's concepts of privacy contributed significantly to the Constitutional assumption of primary importance of the individual, the limited authority of government, and the importance of private property.[1] As a result, several specific protections for various facets of privacy were added in the Bill of Rights. These include the First, Third, Fourth, Fifth, and Ninth Amendments. Additional protection from English common law was incorporated into state constitutions and statutes.

While a number of 19th century judicial decisions contributed to the development of the legal concept of privacy, modern definition begins with "The Right to Privacy" published in the Harvard Law Review in 1890 by Samuel Warren and Louis Brandeis.[2] The motivation for that discussion was a series of contemporary technological developments: the telephone, the microphone and audio recorder, and the camera that could take "instantaneous photographs." These developments, in the opinion of Warren and Brandeis, threatened the individual's right "to be let alone" under current statutes; however, common law, they argued, secured "to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others," and could provide a basis for expanded protections to cover situations raised by the new technologies.

---

[1] A. Westin, Privacy and Freedom, 1967.

[2] Warren & Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

The first court decision based directly on the Warren-Brandeis position was that of the New York Court of Appeals in 1902 in Roberson vs. Rochester Folding Box Co.[3] The plaintiff sought damages for the unauthorized use of her likeness on a bag of cornmeal, but since no property right or breach of trust was involved, the Court failed to award damages on the basis of violation of privacy, per se. However, the next year the New York State Legislature enacted the first so-called "privacy" statute--criminalizing the wrong done to Abigail Roberson. (The statute is limited to unconsented appropriations "for advertising purposes or purposes of trade.") A few other states followed suit.

The protections for privacy that were slowly being built during the early part of the century were severly damaged by the 1928 U.S. Supreme Court decision in Olmstead vs. United States.[4] The case involved the use of wiretap information obtained by a Federal Agent against a Seattle bootlegger. Justice Taft argued that since the intrusion took place away from the property of the accused and indirectly in the form of telephone wires, there had been no violation of Fourth Amendment protection against unreasonable search. Documents surfacing later suggest that Taft's majority opinion was strongly influenced by his special social concern for "law

---

[3] Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902). 1903 N.Y. Laws ch. 132 §§ 1,2 (presently N.Y. Civ. Rights Law §§ 50-51 (McKinney 1948). The text of this New York statute, headed "Right to Privacy", does not mention the word privacy. (See T. Gerety, Redefining Privacy, 12(2) Harv. C.R.L. L. Rev. (Spring 1977).

[4] Olmstead v. United States, 277 U.S. 438 (1928).

and order" and that the case was perceived in that light rather than in light of the important Constitutional implications for privacy it carried.

The protections for privacy lost in Olmstead were not fully recovered until 1965 in Griswold vs. Connecticut.[5] The case involved a married couple's right to use contraceptives. Writing for the majority, Justice Douglas established the concept of "zones of privacy" into which government may not intrude, basing his argument on the penumbra of the First, Third, Fourth, and Fifth Amendments as influenced by the Ninth Amendment.

While Justice Douglas' argument would appear to establish certain absolute protections, the Court soon backed away from that position. In Doe vs. Commonwealth's Attorney (1976)[6], the Court held that the right of consenting adults to engage in homosexual acts in private is not protected on analogous grounds. While the rights of privacy associated with the state of intimacy would not reasonably be argued to take precedence over protective rights of the whole--as with murder, conspiracy, etc.--the rights of privacy have been argued to take precedence over simple cultural norms when no harm is present.

During that same 10-year period, from 1966 to 1976, six major federal privacy-related laws were enacted:

- The Freedom of Information Act (1966, amended 1974);

---

[5] Griswold v. Connecticut, 381 U.S. 479 (1965).

[6] Doe v. Commonwealth's Att'y, 403 F. Supp. 1199 (E.D. Va. 1975), aff'd mem., 425 U.S. 901 (1976).

- The Omnibus Crime Control and Safe Streets Act of 1968;
- The Fair Credit Reporting Act of 1970;
- The Family Educational Rights and Privacy Act of 1974;
- The Privacy Act of 1974; and
- The Tax Reform Act of 1976.

In particular, The Omnibus Crime Control Act and The Privacy Act of 1974 have relevance for this report. The former addresses the question of electronic surveillance and attempts to establish the actions and circumstances in which those actions can be taken to gain private information about an individual or group. Principles set forth in this Act might, by analogy, be extended to cover interception of data and messages from consumer terminals within a public information utility system. The latter addresses the rights of the individual with regard to personal data contained within federal data banks. While affording significant protections within the limited domain of federal systems, it establishes two important principles that have wider implications. First is the right of individuals to know what information exists in a data bank about them and the right of individuals to have errors corrected. Second is the restriction placed on the aggregation of data by consolidation of data bases or the exchange of data among data bases. Of major importance is the principle indicated in these restrictions that data that might be innocuous when viewed separately may be embarrassing or injurious to the individual when aggregated.

Since 1976, no major federal privacy legislation has appeared. However, two developments warrant mention. The Privacy Act of 1974 established the Privacy Protection Study Commission. This commission addressed issues of privacy, particularly those affected by electronic developments. Those interested in attempting to extend the protections established within federal data banks to the private sector will find the Commission's report a useful background document. The second development is the recently enacted New York State Privacy Protection Act. While also limited to government-held records, it goes even further than the Privacy Protection Study Commission in defining the mechanisms for protection.

This brief legal history of the concept of privacy highlights several fundamental points about privacy. First, our legal codes and decisions do not often directly address privacy, itself. Instead, they virtually always address some other injury resulting coincidentally from infringement of privacy. Second, the Congress and the courts have been slow to respond to new media technologies and the threats they pose to privacy--at a time in the very rapid development in communications and data processing technologies.

Refer to Appendix V. for further legal references.

B. Some Social and Other Definitions of Privacy

While a review of the recent legal history of privacy is useful for establishing what actions have constituted infringement, to understand what is being protected we must look briefly at the concept as it relates to the ordinary

social functioning of the individual. One of the most authoritative contemporary commentators on privacy, Alan Westin, has described four categories of privacy: solitude, intimacy, anonymity, and reserve--which are particularly useful for describing privacy.[7]

Solitude is, perhaps, the most complete state of privacy. In this condition, the individual achieves physical isolation; others may not "sense" him, either directly or indirectly. Such a state probably never exists absolutely, since sounds, smells, and other intrusions are likely to enter the consciousness of an individual reminding him/her that a "public" is not far away. Control of this state lies at the heart of many discussions of privacy; it is ironic, however, that the conscious exercise of that control, so carefully protected by some legal definitions, may be as disruptive to the state of solitude as actual physical intrusion.

Intimacy is the state to which a small group may withdraw so that interpersonal relations and the rules that govern those relations may be determined largely by that group. Relaxation, frankness, sexual interaction are often associated with states of intimacy. Couples, families, close groups of friends are common forms of intimate groups. As was seen above, legal recognition of rights of privacy for various forms of intimacy is quite mixed. Thus, intimacy is an area of privacy where cultural and legal recognitions have been and still are at

---

[7] A. Westin, Privacy and Freedom (1967) and other works cited in this report, Appendix V.

odds in some important respects.

Anonymity is the state of privacy where an individual may be in a public place but not be recognized or watched. Relaxation, freedom of movement, spontaneity are associated qualities. While individuals retain some control over this state, by not calling attention to themselves, true anonymity is not subject to any actual control. That is, passersby may choose not to display recognition, but they cannot control actual recognition. Indirect presence, such as publication of a likeness or even a person's name, can be controlled, of course, and privacy concerns have often been addressed to this aspect of anonymity.

Reserve is the state of selected presentation of the self. The individual, through choice, adopts a certain degree of frankness, manner, personal posture. In an interpersonal sense, this aspect of privacy underlies the individual's right and ability to determine the nature of the relationship between self and another person or group; in a legal context, this aspect of privacy underlies, with several other important concepts, the right against self-incrimination protected by the Fifth Amendment.

There are, no doubt, other states of privacy for the individual; but in these distinctions we can glimpse some of its many manifestations. Important to realize is that privacy does not exist in any of these states but exists in and around them. Solitude is never absolute; thus, complete personal privacy lies beyond any actual physical state. Also, privacy

is highly dynamic. Individuals constantly shift among the various states and levels of privacy. After public interaction, the individual seeks privacy in order to assimilate the stimulae of the day and to prepare for the next phase of public interaction. Because these states are defined to a great extent by the information that is revealed in them about an individual, discomfort occurs when the information from one state follows the individual to another. This is so whether that information is communicated directly or inferred indirectly.

C. Some Privacy Issues Connected with Interactive Home Media

In all, neither the existing legal nor social definitions suffice. On the one hand, the legal cases and secondary reviews are not yet a means to understanding the concept of privacy--not until a formal framework is established to cull out the doctrines established so far. This framework should include those doctrines established in related fields, such as the cases dealing with the privacy issues raised by the computerization of criminal, health, banking, and other personal records. Perhaps when such research is completed, it will show that the privacy issues in these cases are basically no different from the ones associated in this report with interactive home media systems. On the other hand, the social definitions, based on how individuals seem to function in society, do not go far enough to define privacy either. What is in order, probably, is a philosophical analysis that will tie the philosophy of the law with other branches of philosophy to provide us an all-encompassing matrix or framework of privacy today.

What is clear is that the current concept of privacy is widespread and ingrained at the same time as it is not easily definable or protectable.

Without the benefit of an established framework defining privacy--its nature and limits--we have developed some categories of privacy issues to begin to help order thinking on the question. We have identified these four major types of exposure:

- intrusion;
- interception;
- misuse of information; and
- aggregation.

Appendix III.

THREE MODELS OF INTERACTIVE HOME MEDIA

Appendix III. A. INTERACTIVE CABLE SYSTEMS

Interactive cable systems are an outgrowth of the conventional one-way cable delivery system for TV. Instead of transmitting a signal only "downstream" from the signal source to the viewer, they are able to transmit some form of signal originating at or near the receiver back "upstream" to the head-end where it is usually received by a monitoring computer. The field is currently dominated by the Warner-Amex Corporation's Qube system. But the recent franchise award to Cox Cable Corporation to wire some 125,000 homes in the Omaha area for interactive service and the entry of AT&T into the bidding suggest that the field will develop quite rapidly in the next few years.

Because it is currently the largest, most developed of the interactive cable systems, Qube will serve as our case study for this technology.

Of all the emerging interactive home media, Qube has probably received the most attention in this country. Qube is the trade name for the interactive cable system developed by Warner-Amex, a recently formed corporation linking Warner Communications and American Express. The only currently operating Qube system is in Columbus, Ohio; however, installations are underway in Cincinnati and Houston, and the Corporation has recently won the franchise for Pittsburgh.

In spite of wide public attention, detailed technical information about Qube is difficult to obtain. Sources for this report are the published literature (the NAB library

maintains a file of most published materials on Qube), an NTIA report prepared by Martha Johnson-Hall, Qube-supplied background and press materials, and information obtained through personal interviews. During a one-day visit to Columbus we talked with the following people:

- Larry W. Wangberg, VP and General Manager;
- Miklos B. Korodi, Senior VP, New Business Development;
- Scott Kurnit, Director, Programming and Production; and
- Richard Guarino, Manager of Systems.

1. System Overview: QUBE

The system may be divided into four major components:

- programming services;
- head-end computers;
- cable transmission system; and
- home terminal and console.

Qube, Columbus, offers 30 channels divided into three groups of 10 channels each:

- television;
- community; and
- premium.

The television channels are the usual cable mix of local network and PBS stations, several out-of-town independents, a news service, several public information channels, and Qube's "flagship" channel--Columbus Alive. For an additional fee, the subscriber may gain access to the community and premium blocks of channels. The community block carries a variety of focused channels: children's programming, sports, intellectually sophisticated features, news/weather, consumer information, live Congressional coverage., religious programming, and credit course material. The premium channels are a pay-TV block containing five general audience movie channels, a "drive-in" movie channel, an adult films channel, and a pay instruction channel. While Qube is using state-of-the-art micro-computer controlled video tape drives as programming sources, this segment of the system is conventional and poses no new privacy issues; consequently, attention will be focused on the other three subsystems.

The aspect of the system that makes Qube unique is the interactive communication between the head-end computer and the microprocessor-driven home terminal. This technology is currently used in three ways:

- viewer response;
- pay-TV billing; and
- home security monitoring.

Viewer response, as well as channel selection, is provided through the separate hand-held console. This device has three columns of 10 buttons each--for channel selection--and a fourth column of five buttons for responses. At designated times in the programming material--primarily on the Columbus Alive channel--viewers are given the option to respond by pressing one of the five buttons. These responses are transmitted upstream over the cable system, collected by the head-end polling computer, and used for tabular or sales purposes. This polling technique can also record the channel currently being watched and is used in this way for billing of the pay-TV services.

Under a separate agreement, the consumer may elect Qube's home security service. In this case, a home security terminal is installed to monitor a variety of sensors: smoke, fire, sound, movement, as well as a manual medical alert device. When activated, these devices send upstream messages, analogous to hand-console signals, which are received by the polling computer. A designated series of actions is then initiated.

These interactive services pose a variety of questions pertaining to privacy. In many instances these derive from potential exposure of information within the system. (Refer to the "Technical Description" section of this report for system details and for discussions of individual exposures within the context of the system as a whole.)

2. Technical Description: QUBE

The Qube interactive cable system may be divided into the following three subsystems, for purposes of description:

- head-end computer(s);
- interactive cable transmission system; and
- the home terminal and console.

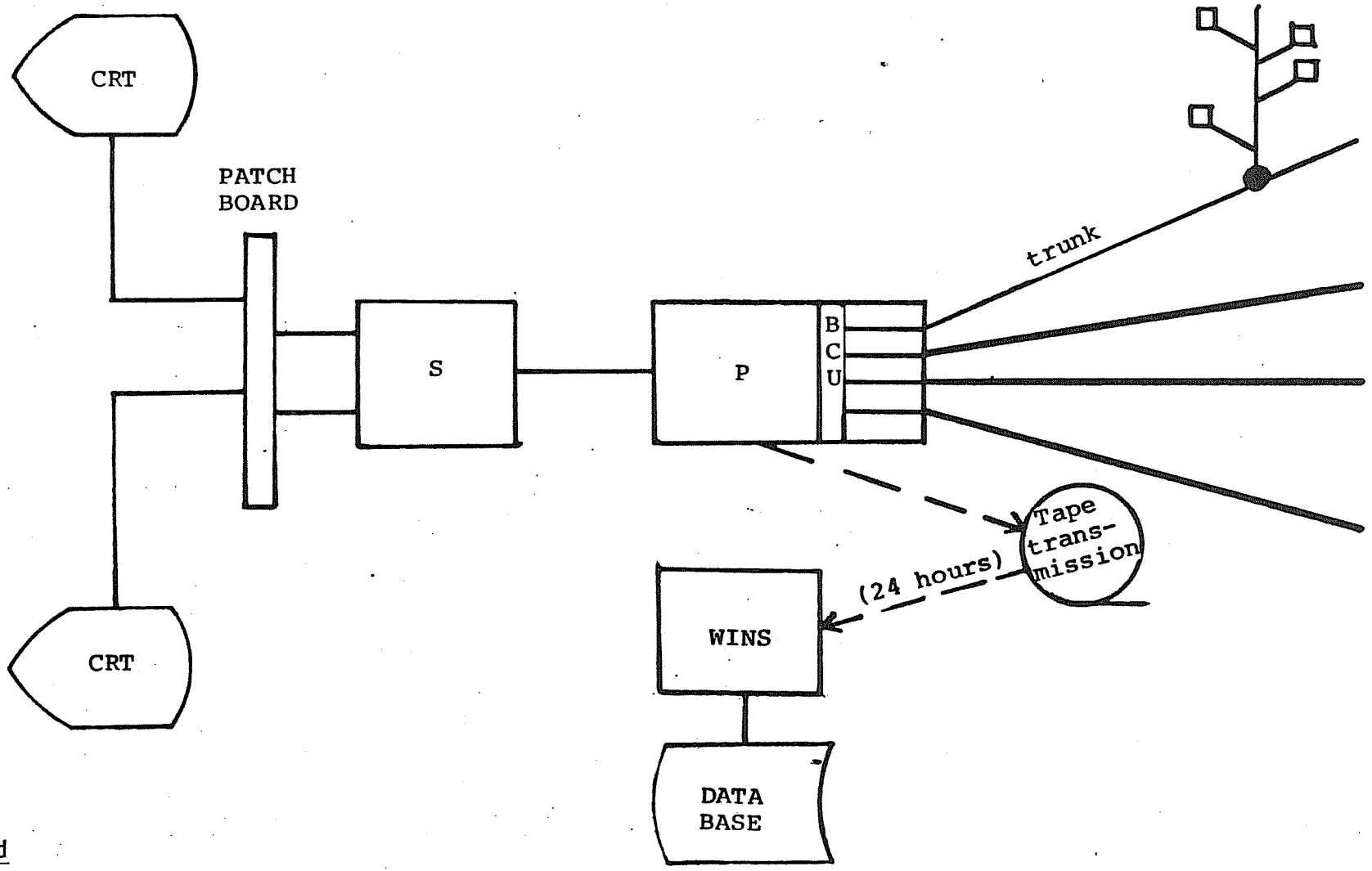
Head-End Computer(s)

The head-end "computer" is actually a group of three individual computers. Qube uses Data General Eclipse S-200 machines--large 16-bit multiprocessing minicomputers each with 256K bytes of main storage. The system employs Data General's standard RDOS operating system, but each computer is controlled by software developed by Qube. The system is configured as shown in Figure 1. (Also, see Glossary, Appendix VI.)

The polling computer (P in Figure 1.) performs one primary function. Using a list of terminal codes or addresses--one unique code for each home terminal--it runs down the list from top to bottom and records the status of the home receiver and the console keys. Indicated are the on-off status, the integrity of the receiver, the channel being viewed (if the set is on), and the last response button pressed (if a response poll is underway). This same polling technique is used for the security system; however, when any alarm condition is received, the system repolls that address to confirm the message before taking the action required.

In the case of a confirmed alarm, the system generates an interrupt condition, notifies an operator through various

Figure 1.



Legend

CRT = Cathode Ray Tube Terminal
BCU = Bi-Directional Control Unit
P = Polling Computer
S = Studio Computer
WINS = Warner Information System

computer room alarm devices, and retrieves and displays on a computer room CRT terminal the household address and any additional user-supplied information (such as a medical history, special architectural features, or hazardous materials) that the user wishes to have conveyed. The operator then notifies the appropriate authorities, conveys this information, and performs any other contingent tasks designated by the user. Anticipated in the near future are direct links to hard copy terminals in fire, police, and medical facility offices.

Under normal conditions, when no security alarm exists, the polling computer passes its data via an input-output link to the studio computer, S. The S computer, as currently defined, performs some eight tasks on a time-sharing basis. These include controlling the CRT's for polling and the security system, performing tests and diagnostics to maintain the integrity of the system, gathering statistical data on viewer selections, and compiling data records of individual use of the premium channels for billing purposes. The records of individual use of the premium channels are gathered over a 24-hour period and transferred via an independent magnetic tape to the third computer once a day.

The S computer also provides operator control of the system. This is done through the CRT terminals. These terminals are located primarily within the same building as the computer system and are, thus, secure within this context. However, dedicated lines to the system do exist between this

facility and the administrative and service locations, approximately a mile away; and there is support for dial-up terminals (CRT's). All such connections pass through a physical patch board so that any terminal outside the physical building must be specifically linked to the system by an operator.

The third computer in the configuration, the Warner Information System (WINS), performs all billing as well as other administrative services. As indicated in Figure 1., this system does not have a direct data link to the P and S machines but, rather, receives data via a transferred magnetic tape. It is within the WINS system that user address codes are matched with actual names and addresses. Itemized bills are compiled for premium channel selection and sent out on a monthly basis; these records are kept for some nine months for routine business purposes, such as verifying itemized charges. Summary data, not containing individual records, are kept indefinitely for programming and marketing purposes.

The three-computer configuration offers the obvious advantage for security and privacy purposes of separating the polling function, where individual viewing activity is recorded and accumulated, from the billing function, where user codes and accompanying data are linked with actual names and addresses. This design, however, is based on financial rather than security considerations. In future systems, a single Data General Eclipse C-350 system will replace the

current three-machine system. While logical or software security precautions will be added, the benefit of actual physical separation will not be retained, according to current plans.

Cable System

Qube, Columbus, uses a single cable transmission system based on an hierarchical tree design. The cable system is connected by multiple trunks both to the programming sources, clustered in an adjoining room within the secured area, and to the P computer. Within this basic design, Qube has introduced three primary developments or innovations: improved amplifiers and filters, an addressable bridge gate controller for regulating upstream transmission, and an addressable "gate switch" at the home terminal that can block reception of selected channels. While the last is, technically, a development within the terminal, it will be discussed here since it functions as the last stage of the transmission-branching design.

The amplifiers and filters, developed under a joint venture agreement with Pioneer of Japan, are of most interest for proprietary purposes than for privacy purposes. The current design supports 300 MHz, but the design being used for Houston is expected to support 400 MHz, thus raising the number of channels carried per cable by 15 or so. This advance, while significant, is dwarfed by the fact that Cincinnati will be a two-lead system while Houston will add a third lead down to certain designated institutions. This

third lead can support, through multiplexing, a large number of both narrow and wide band transmissions originating at numerous points throughout the system. This development could lead to expanded use of the system to transmit messages to and from consumers. In turn, expanded message transmission could raise additional questions regarding security and privacy.

Of more significance from the standpoint of interactive communications are the bridge gate controller and the terminal gate. The bridge gate controller is located at each node in the system and each has an identifiable address that can be referenced by the head-end computer. The controller can be set to either block or to pass upstream responses. It is this facility that permits "narrowcasting". The head-end computer can set the controller in either state thus permitting upstream responses to come from only designated portions of the system. The most widely publicized instance of narrowcasting was the Upper Arlington town meeting where the Planning Commission posed questions to residents within the area and received responses from them, but only from them.

The terminal gate, actually part of the home terminal, works in reverse of the bridge gate controller at the node. It can be set by the head-end computer to block reception of one or more specific channels. Thus, for narrowcasting, the system is configured a few minutes before broadcast time so that only the terminals designated can view the channel involved. It is used routinely, however, in several other contexts: to block reception of the optional premium and

community channels for users not subscribing to those services and to block the adult movie channel for those who do not wish to receive it. (At the subscriber's request, a key-lock is provided in the terminal that can be controlled by the household to block the adult channel.)

Home Terminal and Console

The cable connects in the home to a separate terminal, controlled by a four-bit microprocessor. In turn, the terminal is connected by a cord to the push button selection and response console and to the television set. While channel choices are indicated on the console, actual selection is done by the terminal and the signal fed by cable to the TV set through channel 2.

The primary distinction of the Qube terminal system is its recognition and response capabilities. Three to four times a minute, the polling computer transmits over the system a call to each individual terminal through its numeric code. The exact format of the command structure is regarded by Qube as proprietary, but in form it consists of several start bits, the hierarchically structured terminal identification code or address, a six-bit command, and several stop bits. Recognizing its "name", the terminal interprets the specific command ("are you on or off?", "what channel is on?", "what was the last response button pressed?", "are you OK?", etc.) and then constructs and transmits back upstream the information requested. Having received and recorded that information for that terminal, the head-end computer polls the next terminal

on the list, etc. In the Columbus configuration, the message returned can be inferred to be rather rudimentary; however, under development is a terminal containing an eight-bit microprocessor. The Cincinnati system will use standard eight-bit ASCII codes and it is anticipated that the Houston system will use protocols supporting variable, instead of fixed, length message formats. This last development could lead to some form of message transmission using standard alphabetic coding.

The security terminal works in an analogous way. It is linked to the cable via a split above the home TV terminal cable connection. In turn it is connected to the three categories of sensors that are installed in the home. For security, sensors include ultrasonic motion detectors, pressure sensors for placing under rugs, infrared photoelectric cells, door and window sensors, as well as direct call buttons. For fire, sensors are standard heat and smoke detectors. For medical emergencies, sensors are direct call, both fixed and a small portable battery-operated unit carried on the person. In the current system, the security terminal is polled every 10 seconds (twice as frequently as the TV poll) and responds with an all normal status or the category of alarm that has been enacted. The poll is repeated to verify all alarm responses. A verified alarm "interrupts" the system, which, in turn, retrieves the name and address of the householder and any special instructions provided. Response at Qube is as described above in the "Head-End" section. In future

systems, more detailed information will be transmitted, identifying where in the building motion, smoke, etc. was detected.

3. Privacy and Security: QUBE

Those interviewed at Qube see protection of privacy as in their self-interest, since virtually all revenues are derived from the consumer. That position, however, appears to be part of the working "atmosphere" of the Corporation and has not, so far as we can ascertain, been codified into an actual, comprehensive written policy. In general, Qube has exercised precaution against breach; however, since this is a fast-developing technology, we will comment on portions of the system where potential exposure may exist. We will also comment on a potentially problematic relationship that could develop between subsidiary and parent corporation.

From the point of view of reception, the primary issue we foresee is the undesired reception of objectionable or unwanted programming material. Since Qube offers as part of its pay service a "drive-in movie" channel and a sexually-oriented "adult" channel, some viewers may regard their own inadvertent exposure or the exposure, inadvertent or intentional, of children in the household to this material as an invasion of privacy. However, Qube offers two safeguards: the viewer may select to have the adult channel blocked entirely from reception or they may have a special terminal installed that has a key-lock that controls the adult channel. These precautions taken by Qube seem reasonable and adequate for unwanted exposure to the adult channel.

A somewhat related issue is the possible misuse of buying services offered by Qube to its viewers. At various times

goods and services are offered for sale; the viewer effects a transaction by pressing one of the console keys. While a brief period is given for the viewers to change their minds, no provision is made for countermanding selections made by children or for slower-developing afterthoughts. While such service is a boon for some viewers, particularly the handicapped, it is an area of potential concern.

From the point of view of transmission, there are several areas of potential exposure. Currently, three types of information are generated: viewing choices, viewer responses, and security information. All three types could be sensitive. Viewing choices and viewer responses could be embarrassing or damaging outright; but, more subtly, patterns of selection could be used improperly. Two examples illustrate this point. During the McCarthy era, library circulation records were used as incriminating "evidence"; an obvious analogy exists for the potential misuse of TV selections. Second, patterns in viewing and buying habits could be used to form "psychographic" profiles of a household. Such profiles could be used to devise marketing strategies to which the members of the household are particularly vulnerable; of more general importance, however, is the privacy issue of the individual's or group's perceived right to control the information known about that individual or group. (See discussion of the concept of privacy, above.)

Information derived from security devices has obvious privacy implications. Under the current design, all analog responses are converted to categorical states--fire, medical,

or intrusion alarms--and a digital code transmitted. Under development are refinements to make the information more precise--e.g., the exact location in house from which a sensor is activated. Under development are a variety of other information-generating devices and services. These include monitoring and response equipment for energy-using systems, electronic funds transfer, and eventually message transmission and information retrieval services. Thus, information with varying degrees of sensitivity will be collected in the home and transmitted upstream through the cable system.

Attached to each upstream message is a code identifying the terminal from which it originated. Once this message passes the first bridge gate controller and goes into the trunk system, it is blocked from any further downstream exposure. (See "Technical Description: Qube" for details.) Below the first bridge gate controller, however, are linked as many as 256 terminals. While quite weak, the message signal would flow back down from that node to all the other terminals. Of course, the terminals are designed so that they normally ignore such a signal, but the possibility exists of using a specially-designed terminal to intercept these signals and to eavesdrop. The difficulty of designing such a device, however, makes this kind of activity improbable. Additionally, the nature of the information that could be derived currently would hardly seem to justify the effort of the impropriety; should full message capability be added in the future, however, this exposure may become more meaningful for some individual and corporate

subscribers. The problem could be eliminated by placing a gate below the branch rather than above it to block leakage to other terminals connected to that node. This feature, combined with a microprocessor-driven scrambler, could be marketed as an additional security option for those customers who feel they need this extra measure of confidence.

Once the signal is in the trunk transmission system, it is blocked from any further access at a receiver node. Physically, exposure in the cable system, proper, is analogous to exposure in a common carrier system. Legally, protection against intrusion or eavesdropping afforded common carriers of voice communications has not been extended to cable systems and data links. As these latter grow in number and as they begin to carry personal information that has analogous sensitivity, a review of common carrier protection against unwarranted access to data links--as they relate to interactive cable systems--should be considered.

Once the information obtained from a home terminal is received by the polling computer, there are four basic categories of exposure that must be considered:

- improper access within the secure area,
- improper access via a communication link,
- unnecessary use of information by Qube, and
- forced access to information by a source outside of Qube.

Improper access within the secure area of an interactive home media system poses no new problem; the problem has been long recognized within defense and other secure computer

facilities. Note that this industry shares the same problems of confidentiality with computer room operators and other authorized personnel. Safeguards found effective for secure and classified systems should be adequate in this area, as well.

Qube has initiated a system that provides four major precautions. The area is physically secured by a magnetic card lock system such that only authorized personnel may enter the area. Second, to use a terminal to access the system requires double passwords (known only to authorized operators) for the polling and security functions, and triple passwords that are changed every day for the record keeping function. Third, instructions for conducting a poll or accessing polling information are known only to a small group of approved operators; documentation is physically secured. Finally, all viewer response polls must be approved in advance by the Director of Programming and Production. For approved viewer response polls, the viewer must be informed through the programming content that a poll is being conducted and given the option to participate or not.

Improper access through a communications link would occur should improper use be made of a remote terminal connected to the system--either by a hard-wire or dial-up port. All terminal connections (hard-wired or dial-up) come through a patch board and are manually linked to the system. Operators within the secured area are instructed to make such connections only to known, approved individuals within the organization.

Unnecessary use of information by Qube means use of subscriber records on an individual basis other than for billing purposes. Qube's policy and responsibility are spelled out in the contractual agreement with the subscriber. (See sample contract below; note, especially, item three of this agreement.) Qube may and does develop aggregate statistical data for market analysis. Individual records, we were assured, are used for no purpose other than billing. Such records are retained for a period of nine months, to resolve any disputed claims, and then destroyed. (Of course, in this and similar systems, there is as yet no outside way to guarantee this limited use.)

Privacy and fair market issues may potentially be an issue here, given the diverse nature of the parent corporation, American Express. Aggregate marketing data with rough demographic correlation by neighborhood can be generated. It is reasonable for Qube to use such data for programming purposes. Not clear is whether the parent corporation, American Express, will have access to that information. If it does, the question to be considered is the market advantage for the parent corporation that might be extended to other sectors of business activity.

Perhaps the most significant exposure lies with forced access to Qube records. This could take place if Qube records were subpoenaed by a judicial source, most likely on the state or local levels. Such a case did arise recently, as the attached news accounts show. In that case, a local movie

house operator was arrested on obscenity-related charges stemming from the showing of two adult movies, one of which was shown on Qube's pay adult channel. The defense attorney based the defense on the grounds that the films did not violate community standards of obscenity; and had subpoenaed Qube's records to establish local viewing patterns of such films. While Qube vigorously defended individual viewing records, it did supply general viewing statistics on both the individual film in question and the patterns of use of the adult channel. While Qube asserted it would fight access to individual records all the way to the Supreme Court, not clear is whether other interactive cable media corporations would resist such access. Legal access to individual records of viewer selection is clearly an area for review--to determine whether regulatory and, perhaps, statutory address are required.

AGREEMENT FOR QUBE™ SERVICE

As requested by you, the Subscriber, QUBE has installed its unique, interactive Cable TV Terminal and Console (along with associated connection lines and materials) in order to provide QUBE service. In consideration for the installation and provision of QUBE service, you hereby agree as follows:

1. Subscriber will have the opportunity to interact with QUBE programming as, for example, by registering opinions, ordering programs and other products, and participating in game and other shows. Such interaction is entirely voluntary and is completely within Subscriber's own control.

2. Unless otherwise agreed, Subscriber will be billed for (i) installation of QUBE equipment, (ii) basic monthly service and (iii) individual "premium" channel programs which Subscriber watches for 2 minutes or more. QUBE charges are payable promptly upon receipt of the monthly bill.

3. Subscriber's "premium" channel program selections will be recorded on a computer printout. Such records shall be kept strictly confidential except for purposes of servicing Subscriber's account.

No other individualized records will be developed of either viewing selections or interactive responses unless the Subscriber has been advised in advance and given adequate opportunity not to participate.

4. Subscriber may discontinue QUBE service at any time.

5. QUBE's agreement to provide service to Subscriber in advance of payment is conditioned upon a reasonable showing that Subscriber is in good financial standing. (QUBE may verify Subscriber's credit standing with a consumer reporting agency such as the Credit Bureau of Columbus, Inc. in accordance with applicable laws. The Ohio laws against discrimination require that all creditors make credit equally available to all credit-worthy customers, and that credit reporting agencies maintain separate credit histories on each individual compliance with this law.)

6. The QUBE Terminal and Console are, and remain even when installed, the property of QUBE. If Subscriber's QUBE service is discontinued for any reason, the Subscriber agrees promptly to return the Console and Terminal to QUBE by permitting a QUBE representative to enter the premises where the Console and Terminal are located for the purpose of removing same. (QUBE shall not be liable for wall holes, etc. which may remain after removal of equipment, except for damage caused by QUBE's negligence).

If, upon discontinuance of service, the Subscriber does not promptly return the Console and Terminal to QUBE, then Subscriber shall be obligated to pay to QUBE the amount of $250.00, which Subscriber and QUBE hereby agree is the value of the installed Console and Terminal, plus any additional charges owed to QUBE.

7. Physical damage to the Terminal or Console caused by the Subscriber, other than that due to reasonable wear and tear, is the responsibility of the Subscriber who shall be obligated to QUBE for the reasonable costs of repair or replacement. Subscriber agrees to provide reasonable access so that the Console and Terminal may be repaired or replaced.

8. QUBE shall not be liable for (i) the quality of any merchandise (purchases, prizes, etc.) received by Subscriber in connection with QUBE programming; (ii) the representations or warranties made by the Seller and/or manufacturer of such merchandise; or (iii) damage or injury if any, resulting from the use thereof.

9. Subscriber is aware that theft of cable television service and/or property or willful injury, destruction or alteration thereof is punishable under Ohio Revised Code (Section 4933.42) by fine of up to $500.00 and/or imprisonment of up to 60 days and under Columbus City Code (Section 2305.13) by fine of up to $1,000.00 and/or imprisonment of up to 6 months.

Adult Theater's Lawyer Wants Data On Cable Sex Films

The attorney defending a local adult movie theater wants to know how many people in Franklin County are watching sexually oriented movies on cable television.

Cable TV officials protest that the rights of their subscribers must be protected, but a Municipal Court judge Friday agreed to allow attorney Laurence Sturtz to subpoena officials of both Warner Qube and Coax Cable TV to testify on the matter.

THE UNPRECEDENTED move raises a myriad of legal questions about the right to privacy of a viewer watching such films at home, cable officials and some legal authorities said.

In what is regarded by his opponents as a shrewd maneuver, Sturtz is trying to show that sexually oriented movies exhibited at the Adult Theater, 1320 S. High St., may not violate community standards of obscenity if such movies have garnered great popularity among cable TV subscribers.

The case stems from the March 14 arrest by Columbus police of four employees of the theater on obscenity-related charges linked to the showing of the films *Taxi Girls* and *Captain Lust* Feb. 28.

STURTZ'S DEFENSE is based on a 1973 U.S. Supreme Court ruling stating that in order for a work of art to be judged pornographic, the material must violate contemporary community standards.

As a result of the court order he obtained Friday, Sturtz plans to subpoena Qube and Coax representatives to give videotaped depositions May 20 and 21.

The order, signed by Municipal Judge James C. Britt on behalf of vacationing Judge Dale Crawford, allows Sturtz to subpoena Qube for a copy of the same *Taxi Girls* movie which his clients are charged with showing, and to question the company about viewership statistics on that film and other sexually oriented movies it has shown.

STURTZ WANTS to gauge the extent of the popularity of cable TV's sexually oriented films by admitting Qube and Coax viewership data into evidence.

Only Qube now offers sexually oriented film on a pay-TV channel. Coax offered sex films from 1974-79 on a pay-TV service called Tele-Cinema that is now defunct.

Just how much data can be legally obtained from the firms remains to be determined. Lawyers and cable TV officials interviewed Friday said the names of cable TV subscribers should not be used in court.

LEO BRENNAN, Coax general manager, said he could understand the use of statistical data in a courtroom in order to determine a community obscenity standard.

"But," Brennan said, "I can't imagine being in a position of divulging a viewer's name. I have to believe there is no way we would want to get into anything like that."

Please See VIEWERSHIP On A-3

Continued from Page 1

When informed of the judge's order, Qube's director of operations, Larry Wangberg, said, "There is no way we would give out any individual information. We have a policy to protect our subscribers."

Any effort to subpoena subscribers' names would be fought by the TV company, Wangberg said.

WANGBERG ALSO said he was not aware that *Taxi Girls* was ever shown on the Qube cable. Judge Britt said the cable companies will be allowed to request a hearing to contest the subpoenas.

City Prosecutor Ronald O'Brien said the statistics or the films are neither relevant nor admissible in the trial.

Stan Laughlin, a professor of constitutional law at Ohio State University and a member of the state board of the American Civil Liberties Union, said because the Supreme Court has made a sweeping concept like "community standards" relevant in court, a wide range of evidence — including cable TV viewership data — can surely be admitted into evidence.

HOWEVER, EVIDENTIARY discovery procedures can go overboard as far as using subscribers' names are concerned, Laughlin said.

"It bothers me that there is a privacy interest that can be invaded here. . . . I think I could make an argument (against using names)," he said.

Judge Crawford will hear the case in a jury trial scheduled for June 9.

THOSE CHARGED with two counts each of pandering obscenity, relating to the films *Taxi Girls* and *Captain Lust*, are Dean L. Darling, 38, of 690 Thurber Dr., Apt. A-6; Domenic Suriano, 43, of 518 E. Town St.; and Raymond J. Satola of 1190 Amanda Northern Rd., N.W.

Edward Demmler, 39, of 1025 E. Jenkins Ave. faces one count of complicity to pandering obscenity.

TUES., JUNE 10, 1980 F Columbus Dispatch B-7

Qube To Give Sex Film Data

By Mark Ellis
Of The Dispatch Staff

The Warner Qube cable television company has agreed to provide an attorney with data on how many of its subscribers watched sex films.

The attorney is defending a theater manager accused of pandering obscenity.

The information could be used by jurors to help define community standards of obscenity.

SCREENING OF the sex films *Taxi Girls* and *Captain Lust* was scheduled at Studio 35, 3055 Indianola Ave., Tuesday for the jury hearing the case against an adult movie theater employee.

Jurors were selected Monday and Tuesday in Franklin County Municipal Court to hear the city's case against Domenic Suriano, 43, of 518 E. Town St. He is charged with two counts of pandering obscenity in connection with his March 14 arrest for showing the two movies Feb. 28 in the Adult Theater, 1320 S. High St.

Chief Prosecutor Ron O'Brien said he has dropped similar charges against Edward Demmler, 39, of 1025 E. Jenkins Ave.; Raymond Satola of 1190 Amanda-Northern Rd. N.W., and Dean Darling, 38, of 690 Thurber Dr., Apt. A 6. Satola was the projectionist, Demmler was the ticket-taker, and Darling a maintenance man, O'Brien said. Suriano managed the theater.

DEFENSE ATTORNEY Laurence Sturtz had issued subpoenas to two local cable television companies in connection with the case. Qube and Coax Cable TV were asked to provide information about sex film viewers.

Qube has agreed to provide the number of viewers of sex films for this year and the number of viewers for a cut version of *Taxi Girls* sold over cable.

Citizen-Journal
Friday
June 13, 1980

Manager of theater wins in smut case

By HARRY FRANKEN

Domenic Suriano, manager of the Adult Theater at 1320 S. High St., was found not guilty Thursday of pandering obscenity.

The eight jurors had underlined the phrase "contemporary community standards" on a blackboard in the jury room, indicating they thought the community did not object to sexually explicit movies when shown to persons who chose to attend adult theaters.

City Prosecutor Ronald J. O'Brien said he believes the issues were fairly and completely presented to the jurors, and that they had made their decision on the evidence.

"I would say we had a very conservative jury," O'Brien said. "I don't know that we could ever expect to present these issues to a jury that would give them fairer consideration."

O'Brien said, however, that a decision had not been made on whether to proceed with the trials of seven other defendants on the same issue. The charges are pending against two other theaters and several adult bookstores.

"We don't set the community standards; we don't want to set the community standards," O'Brien said. "Apparently the jury spoke as to the average community standard. If there are any folks in the community who feel the jury did not speak for them, they should let that be known to the appropriate law enforcement agencies, specifically in Columbus, the Vice Bureau."

Robert Muetzel of 31 Eastgate Drive, a member of the Coalition of Concerned Citizens that led a public campaign against the Adult Theater, said he was disappointed by the jury's decision.

Continued on Page 9, Col. 1

Manager of theater wins obscenity case

● From Page One

"They spoke of contemporary community standards," Muetzel said. "That upsets me, because they aren't my standards, and they aren't the standards of most people I've talked to. To me, what the jury said was that type of thing is representative of what people want to see, and I can't believe that."

In the trial before Judge Dale Crawford, jurors were told by defense attorney Laurence Sturtz that sexually explicit movies and books are readily available in the county.

One witness said QUBE cable television in Columbus broadcast one of the movies involved in the suit and that 10,655 sets were tuned to the showings.

It was also testified that up to one-fourth of the QUBE viewers watch the adult entertainment offered by the station.

Explicit movies were viewed by the jurors in the courtroom and in a visit to the Adult Theater.

Crawford had refused to admit into evidence a petition bearing 4,800 signatures of persons who objected to the availability of obscene materials.

In the courtroom when the verdict was returned was Judge Richard Ferrell, who has drawn six of the pending cases.

Suriano, contacted at the Adult Theater Thursday night, said he is pleased with the decision.

"I think it's just a message that most adults feel the movies are OK for adults, and they don't feel that government should interfere," Suriano said.

Appendix III. B. INTERACTIVE VIDEOTEX-TELETEXT SYSTEMS

The second type of interactive home media--videotex and teletext systems--offers the user formatted pages of information displayed on a TV set using a conversion unit, installed separately or incorporated in some of the newer specially designed TV receivers. The field is marked by several significant factors: strong interest, rapid development, technical instability, and the lack of firm definition. These factors are highly interrelated and may indicate a very rapid rate of development in the near future accompanied by strong competition among the various designs.

Because the field is so dynamic, it is difficult to establish firm descriptive categories. Often the name associated with a particular videotex or teletext system is more accurately associated with a set of coding protocols (the design of the message record and the display). Consequently, a given system can rapidly "develop" right through technical distinctions between videotex and teletext--such as the transmission mode--that have been useful in the past. For example, in one implementation Telidon is a one-way teletext system using a portion of the broadcast TV signal for data transmission; in another, it is an interactive videotex system using the telephone network. Thus, one can associate "Telidon" not so much with a given physical system as with the design protocols that lie behind the system.

Below are several examples of interactive videotex-teletext systems. The design characteristics as well as the

actual details of implementation are provided for each. Included are some systems that are currently one-way but whose design supports interactive access and whose developers appear to be moving in that direction. These three home media (consumer-oriented) interactive systems are discussed: Prestel (British), Telidon (Canadian), and Antiope (French). We have chosen these particular systems for two reasons: they reflect the major design distinctions among such systems and they appear to be the systems most likely to have substantial penetration in the U.S. in the near future.

NOTE: Because this technology--unlike interactive cable and general purpose consumer-oriented computer utilities (discussed in the next section)--is not yet operational on a public basis in this country, we have also provided brief overviews of their implementations in Britain, Canada, and France.

In developing these studies, we have reviewed the published literature, various sales and press kits offered by the respective agents, and the files of several private and governmental collections, including the libraries at the National Telecommunications and Information Administration and the National Association of Broadcasters. Additionally, we made on-site visits and talked with the following individuals:

Prestel

- R. Barry Williams, Consultant, Logica, Inc.
- Richard H. Veith, Ph.D., Consultant, Logica, Inc.

Telidon

- John H. Syrett, Project Manager, Ontario Educational Communications Authority
- Tom Thorne, Project Officer, Telidon and Education Project, TV Ontario

Antiope

- Gary D. Rosch, Staff Counsel, Antiope Videotex Systems
- Marvin Segel, Marketing Manager, Antiope Videotex Systems

1. System Overview: Interactive Videotex-Teletext Systems

Videotex-teletext systems display on a TV screen pages of information selected by the viewer. Pages are typically 40 characters wide and 20-25 lines long. All systems have provisions for displaying graphic illustrations as well as text; they differ rather widely, however, in their basic approaches to graphic display and in the degree of image resolution.

A specific image is selected for viewing through some type of console, ranging from a hand calculator-sized numeric keypad to a full alphanumeric keyboard. Images may be selected by first viewing a general menu, then choosing a succession of "sub-menus" leading down to the actual information frame desired; or one may go directly to the information frame by recalling its unique frame identification number. Lag time between indication of choice and the appearance of a frame is usually about ten seconds.

Information frames are available from a wide variety of industries. These include wire services, newspapers, publishers, retail stores, service vendors, advertising agencies, government agencies, financial transaction corporations, and entertainment corporations. Frames that describe goods or services for sale are usually provided free of charge; others are usually offered for a fee ranging from a few cents to a dollar per information frame. Information may be formatted by the organization itself; but there is a growing tendency for "umbrella" corporations that specialize

in formatting to provide these services under contract. It is the responsibility of the Information Providers to structure their data through menus, sub-menus, and numbering conventions. The primary responsibility for content so far also lies with the Information Provider.

Completed frames are accepted by the controlling corporation, indexed, and stored within the head-end computer(s). Typically, the head-end computer is a medium to large minicomputer (e.g., a 16-bit processor with some 256K bytes of main storage) with large disk capacity (e.g., eight to twelve 70-megabyte disks).

Frames are transmitted to the viewer in one of two ways: either by retrieval of the specific frame selected and transmission over a switchable narrowband link such as a telephone line (videotex) or by broadcast of all available frames over a wideband link such as one or more TV channels or some portion of the channels and subsequent selection or "frame-grabbing" at the terminal (teletext). The latter, of course, is not interactive, but the major systems that offer teletext service either have or anticipate interactive implementation.

While the display unit is the conventional TV set, all systems require a microprocessor-driven terminal/adaptor, either connected to the set externally or incorporated within. Systems differ widely in the sophistication and cost of the adaptor. The difference in sophistication lies largely in the buffering capacity and in the character or image generation capability of the unit. Costs for the conversion apparatus range from a few hundred dollars to more than a thousand.

Individual Systems

Prestel is the videotex system developed by the British Post Office. Begun in 1971, the system went through several pilot stages before being offered to the general public in 1979. While still available only in major urban areas, Prestel has received more actual-use testing than any other videotex system. Currently, the system serves over 5,000 users and offers a data base of more than 150,000 frames provided by some 150 Information Providers. Additionally, Logica, a British consulting firm, is conducting an international field trial in anticipation of providing Prestel services around the world, primarily to businesses but also to individuals; a number of U.S. corporations are participating in this trial.

Telidon is the videotex-teletext design developed by the Communications Research Center of the Canadian Department of Communication. Telidon is as much an abstraction and symbol of national pride as it is a tangible working system. In fact, there are currently two major implementations of the system: a one-way teletext system developed and under field trial by TV Ontario; and an interactive videotex system developed and under field trial by Bell Canada. When one reads the literature or talks with Telidon developers, one is struck by the number of far-reaching goals and the diversity of technologies that are gathered under the term, Telidon. The apparent problem is simplified considerably, however, by the realization that the core distinction is not with regard to

any single total system but the unique (among videotex-teletext systems; not among computer display systems, in general) image-generation protocols that underlie the system(s). These protocols, called Picture Description Instructions (PDI), were designed so that they support both one-way teletext as well as interactive videotex services; they may be transmitted over conventional phone lines, within the vertical blanking interval of a TV picture, over a full broadcast or cable channel, over optical fibers, and, most likely, over other link technologies that may evolve.

Telidon, like Prestel International, will soon be imported into the U.S. With support from the National Science Foundation, the National Telecommunications and Information Administration, and the Department of Education, the PBS station, WETA, will begin a pilot study in the Washington, D. C., area this fall. There are some indications that this test might lead eventually to adoption of Telidon protocols for captioning and teletext services by PBS.

Antiope is a videotex-teletext system developed in France. In 1975 the French government decided to provide every literate French resident with access to a very large repository of information via computer. Antiope is the result of that deliberate commitment. Antiope, as a specific system and as a set of design standards, can best be understood in the context of this government mandate. As a system, Antiope refers to a broadcast one-way teletext system that began commercial operations in 1977. As a set of standards, it refers both to

the language specifications that record display control features as well as alphanumeric and graphic content and to the packet-switching protocols that govern transmission.

To understand the implications of Antiope, one must also consider its videotex implementation--referred to by the name, Teletel. The initial use of Teletel, under Antiope protocols, will be the computerization of the French telephone directory. By 1982, 270,000 terminals will be installed in the Ille et Villaine region free of charge to the subscriber. Using the telephone lines, the terminals can interrogate the data base by name, location, and commercial category; thus, both white and yellow page directories will be replaced, and access by street address will be added. Over the next 10 years, France will phase out all printed directories by installing over 30 million terminals for its subscribers.

Once again, the implications go further than the primary use. The French, essentially, are using the telephone project as a strategy for placing videotex equipment free of charge into the vast majority of households and businesses. Since the inverted file software is general, a large number of other types of data may be expected to be offered in addition to directory information. Thus, the French have begun the first systematic effort to realize the "wired nation" concept of near total computer-access penetration that has been the object of much recent speculation in other countries.

Antiope is important for U.S. interests, as well. CBS, after a trial project using teletext Antiope at its St. Louis

affiliate, KMOX, has filed a petition before the FCC to set standards for U.S. teletext transmission based on Antiope protocols.

2. Technical Description: Videotex-Teletext Systems

A. Prestel

Prestel information frames are prepared by independent Information Providers. Frames are assembled and linked into the general indexing system of the data base through dedicated UpDate Computers. Frames may be created and edited on-line within the UDC system; they may also be prepared off-line on an intelligent terminal with storage capacity or on the Information Provider's own system and then sent in bulk to the UpDate Computers. The UpDate Computers hardware is a GEC 4082 16-bit minicomputer with 384K bytes of main storage and 12 70-megabyte disks. (See Glossary, Appendix VI.)

The data base is designed as a large tree structure. Each individual Information Provider is assigned a "top" entry point number of three digits and is responsible for establishing menus and other aids to guide the user through its frames. When frames are created, the Information Provider must identify the frames that might logically follow and provide instructions to the user as to what to key to select a particular succeeding frame. Thus, paths through the data are pre-established by the Information Provider, discouraging casual browsing by the viewer.

Actual retrieval of data is provided through a network of local Information Retrieval Computers. Each Information Retrieval Computer is similar to the UpDate Computers system but configured with fewer disks. Each Information Retrieval Computer contains a copy of the complete data base, updated

daily through a high-speed link with the UpDate Computer. The Information Retrieval Computers are housed within telephone exchanges and are designed so that no local operator is required.

The user gains access to the Prestel Information Retrieval Computers through the conventional telephone system. The telephone line is terminated in a dual socket: one that accepts the jack for the telephone and the second that accepts the jack from the terminal for the converted TV set. Transmission over the dial-up link to the Information Retrieval Computers is 1200 baud downstream and 75 baud upstream using a full duplex format that permits simultaneous transmissions in both directions. To establish connection with Prestel, the user must dial the Prestel number, key in an identification code, and then add a password.

The terminal, a single unit, contains within it the modem that interfaces with the telephone line, a microprocessor controller, a memory buffer, a timing controller, and a character generator. This unit is, in turn, connected to the keypad and to the TV set--if it is not in-board. Both the terminal and the keypad/keyboard are obtained by the user from independent vendors. Consequently, a number of different brands are available. Three styles of keypad are currently offered: a numeric keypad, a compact alphanumeric keypad for one or two finger entry, and a full-size alphanumeric keyboard.

Each information frame consists of 24 rows of 40 characters, for a total of 960 display characters, plus 64 control characters

not displayed; each frame record transmitted to the terminal consists of 1024 characters and is stored on disks within the head-end computer as 1K byte fixed-length records. Frame generation at 1200 baud, thus, takes some 8-10 seconds. Frames are sent as a continuous stream of characters using 8-bit ASCII protocols (7 bits plus parity).

Three different types of data are transmitted: control information, alphanumeric characters, and graphic characters or mosaics. The control information, in turn, is of two kinds: general terminal control characters and image control characters. The terminal control characters clear the screen, set various conditions, and control the switching between character sets. The image control characters control foreground and background colors, steady and flashing modes, normal or double height for characters, display and conceal status for characters. The alphanumeric character set is the standard upper and lower case alphabets, the numerals, and common symbols (percent, ampersand, Pound, etc.). The mosaic character set consists of 64 different configurations of six small blocks (three rows of two blocks each) each of which may be either a foreground or background color. Each mosaic occupies the same screen space alloted a character. Using these mosaics as elements, the Information Provider may "draw" various diagrams or other graphic images to accompany its textual message. Switching from one character set to another is done through special escape characters.

Considerable debate has focused on the mosaic approach; Telidon's alphageometric approach, for example, was developed, largely, as an alternative to this method of graphic representation. However, Prestel is currently developing an improved graphic mode whereby the mosaic elements transmitted become increasingly smaller, thus successively increasing the resolution of the image. This is done by transmitting some six to eight additional 1K records to the terminal. Thus, viewers may receive the standard block form (mosaic) image; if more resolution is desired, they may wait while the picture becomes successively clearer in incremental steps every 8-10 seconds until it reaches full video resolution or they may interrupt the process at any point and move to another frame. For example, were viewers scanning real estate listings that contain pictures of the property, they might view the low resolution mosaic image, perhaps let it go through one or two refinement steps, but then interrupt the process at the point that it becomes apparent that the property is not suitable for their needs. On the other hand, those that seem suitable would be allowed to develop to full video resolution. Picture Prestel requires a more sophisticated and more costly terminal, but savings in large-scale integration (LSI) technology have led the British Post Office to conclude that the economics are viable.

As indicated above, control of the frame selection process is through the keypad or the keyboard. Users may follow a hierarchical, branching path down through successive

menus to the desired information frame or they may go directly to that frame if its identification number is recalled. In certain instances, users may also create and deliver a message to an Information Provider, providing they have one of the alphanumeric-type consoles. This is done through special frames that have fields into which users may key information. For example, various firms offer shopping services whereby users may indicate the product desired, their name and address, and a credit card number. The message frame is then stored for the Information Provider who retrieves it and fills the order. Considerable expansion of this type of transaction is expected, including electronic funds transfer and terminal-to-terminal message transmission.

Prestel maintains records of connect charges, the running total of frames selected by viewers, and the running total of royalties due an Information Provider. Records of individual frame selections, per se, are not kept and are, hence, not a matter of concern for Prestel. However, messages or orders are turned over to the Information Provider when viewers complete a message form. Prestel does not control what the Information Provider does with this information, how long it is kept, or how it is aggregated.

B. Telidon

In describing the Telidon technology, we will not go into detail about segments that are analogous to segments in other systems; instead we will concentrate on those segments that are unique or that have not been described already.

At the head-end, two primary distinctions can be noted. First, because Telidon is still in the development stage for all implementations, a smaller number of firms and agencies are providing information frames; hence, the current data base is far smaller for Telidon than for Prestel. (As will be discussed below, this condition will remain inherent, but for different reasons, in the teletext implementation.) Second, frame creation can be done practically only on a specially designed editing terminal. These units currently cost approximately $20,000; advances in the technology and the economies of scale that can be expected suggest that this figure will drop and will not pose any serious disadvantage in the long run. In fact, while alphamosaic images can be created on a conventional terminal, several comparable editing terminals have been developed for both the Prestel and Antiope systems and are likely to become standard equipment for most Information Providers.

Currently, there are two types of communication links being used. Bell Canada is using in its two-way videotex implementation standard dial-up lines. As with Prestel, it has adopted 1200 baud downstream and 75 baud upstream rates as its standard. Modem requirements are also comparable.

TV Ontario is currently transmitting Telidon images embedded within the vertical blanking interval of its normal video broadcast. Because the latter implementation has not been explained and because it determines the practical size of the data base, we will describe it briefly, even though such broadcast systems are currently one-way.

Within the standard 525-line U.S. television signal, lines 1-21 are designated the vertical blanking interval and contain synchronization, testing, and other control information. These lines are not displayed on the set and are, hence, invisible to the viewer. Several of the vertical blanking lines are unused by television and have been adopted for transmission of digital data for teletext systems. Specifically, TV Ontario uses lines 15 and 16 for Telidon data; WETA has added two additional lines; others have proposed setting aside the entire block from lines 10 to 21 for teletext data. Of course, the entire signal beyond the synchronization portion could be employed for unused channels, especially on cable systems.

Using a teletext transmission mode, either broadcast or over a cable, the head-end computer steps sequentially through the data base and transmits each frame. The time it takes to cycle through the data base is the maximum delay the viewer will experience between the time a frame selection is keyed and the time it appears on the screen. The larger the data base, the larger the delay. If one sets an arbitrary maximum permissible delay time of 20 seconds, a protocol using two

lines from the blanking interval limits the data base to approximately 100 frames; relations between other wait times and number of pages are linear and can easily be estimated (200 pages would produce a maximum wait time of 40 seconds, etc.). The average wait time will be half the maximum.

Under these limitations, one can project that for vertical blanking implementations, the maximum practical data base size is likely to be 100-500 frames per available channel. If all 525 lines of an entire channel are used, that figure will rise to a maximum of some 10,000 to 12,000 frames per channel. Given the current size (150,000 frames) of the Prestel data base and the very strong pressures to increase that number, broadcast teletext appears to be quite limited in its long-range potential, although it seems likely to enjoy short-term success.

The major distinguishing characteristic of Telidon is its alphageometric graphic generation protocols. This feature is related to both the design of its language specifications and the graphic signal generation performed within the terminal. Instead of transmitting either a predefined image or an alphamosaic image composed of characters or character-sized color elements, Telidon transmits most graphic images as a symbol sequence defined in terms of primitive geometric shapes (such as point, line, arc, circle, and polygon) accompanied by their intended positions on the screen and their sizes. In turn, the terminal interprets the command and composes the form described, using magnitude and position parameters, and

stores it in a buffer. Successive shapes of characters are added, in any order, until the frame is complete. Then it is displayed. The sequence is more like "painting" the picture than composing it in the rigid line-by-line sequence, top to bottom, associated with the TV raster scan. Additionally, locations are described in a logical data field 4K positions by 4K positions and then translated into the actual field size determined by the resolution of the individual TV display unit. Should higher resolution receivers appear in the future, Telidon frames would not have to be modified to depict images of greater precision. Frame records are variable in length and in many cases can be built up with one-half to one-third the number of bytes required for Prestel's fixed-length records.

Selection by the viewer is through a hand-held numeric keypad linked to the terminal. Using menus in a tree structure, users move through the data base selecting display frames. After keying a selection, they wait until that frame comes around and is displayed. In the teletext implementation, no selection data are generated in the head-end computer; hence, there are no matters of privacy to be considered in that area. However, the WETA trial will use a meter on the terminal that records individual selections to develop a profile of system use.

C. Antiope

Since there is nothing particularly unique about the head-end computer requirements and data base structure, we will concentrate our description of Antiope on the two features of the system that appear to be most important: the packet-switching protocols and the language specifications.

Under the packet-switching concept, records do not correspond to display lines but to arbitrary packages of data that are assembled at the terminal in a buffer, converted into a visual frame by the character generator, and then displayed on the receiver. Under Antiope protocols, each packet begins with a prefix consisting of synchronization information followed by the address of the information (its position in the sequence of all such packets for the frame). Following each prefix is a block of data characters that indicate display information (such as color, size, and blinking) attached to the character or mosaic content. The end of a display line is signaled by special symbols (a line feed and a carriage return) rather than by filling out the line with the character, blank. By freeing the information from the sequence in which it is transmitted, the channel that actually carries the packet can be as broad or as narrow as desired and time division multiplexing can be freely used. This "transparency" of channel characteristics makes the system quite adaptable to developments in transmission technology. While the French seem intent on moving to the two-way standard of Teletel, utilization of full channels on cable systems may make certain

teletext implementations difficult to distinguish from videotex.

A second innovation in Antiope protocols is its language specifications. The close linking of display characteristics with content elements has generated a good deal of debate. Antiope allocates two bytes for each character: one for the display information and one for the character itself. While questions of efficiency are timely and appropriate, they will be absorbed into the relative consideration given to the order of magnitude differences in data base size and one-way versus two-way factors that are central to decisions between teletext and videotex implementations. Of greater long-range consequence is the down-loading capability of alternative "alphabets". While the Antiope character set has been expanded to include accented characters along with conventional characters and graphic mosaics, Antiope also has the facility to down-load to the microprocessor in the terminal other graphic forms to be used instead. Thus, for example, a cyrillic character set can be down-loaded at the beginning of a frame and the display generated in those forms. Using the same technique, high resolution graphic mosaics can be down-loaded that appear to duplicate Telidon's image resolution on conventional terminals. Also being considered is a set of "chirographic" instructions that will permit free movement of the cursor. While the decision whether to implement will be based on the economics of a more sophisticated decoder in the terminal, it offers considerable flexibility in the long run for graphics and might even be able to support animation.

Like Telidon, the Antiope system in teletext mode keeps no individual user selection data. Since the videotex version, Teletel, is not fully implemented, record keeping policy is not yet defined. We have been told, however, that the general European practice of not retaining detailed itemized records will almost surely be maintained.

D. Other Systems

We do not wish to suggest that the three systems described are the only significant videotex-teletext implementations or that they contain all of the imaginative design features. Virtually every industrial nation is experimenting with some form of videotex or teletext system. Often, however, these systems employ, with varying degrees of modification, the design and/or the hardware of one of the three systems described. The primary exception is the Japanese system, Captain.

Captain differs from other systems in one major respect: because of the large number of ideographic characters commonly in use in Japan, it has opted to generate the display pattern at the head-end rather than at the terminal as its primary mode. The character is selected from a large repertoire (over 3,000 are in common use), displayed in one of three sizes, and the entire composed frame transmitted to the terminal. Like Antiope, Captain uses packet-data protocols but the data transmitted consists of actual color dot patterns. By using side-band transmission techniques, they have been able to transmit data at 3200 baud experimentally. Not clear at the present time is the feasibility of using this rate for full-scale implementation. While interesting and innovative in many ways, Captain is unlikely to displace the character-transmission systems that currently dominate in western countries.

3. Privacy and Security: Interactive Videotex-Teletext Systems

Within the home or office of the viewer, issues of privacy can be identified both with the information received and with the information transmitted upstream. Issues pertaining to reception are of two major types: unwanted exposure to obscene or other offensive content and inadequate differentiation between factual and persuasive content. Growing out of a broadcast context, Qube (our case example for interactive cable systems) regards programming as an integral part of its responsibility. Qube does not, of course, control the content of the stations carried; but it does control the content of some 20-odd channels for which it provided programming. Videotex-teletext systems, on the other hand, see themselves as analogous to common carriers; consequently, they have consistently avoided any direct control over frame content. They have, instead, passed responsibility for content, in accord with accepted standards for libel and obscenity, to the individual Information Provider. If the Prestel experience is duplicated in this country, this would lead to hundreds of Information Providers providing frames of their own design and in accord with their own interpretation of accepted standards of content. Unlike Qube's "adult movie" channel that can be rejected outright or controlled by a key, videotex-teletext systems do not currently offer demarcation of frames that some viewers may find offensive.

An area warranting further study is the failure to mark frames created by advertisers and frames that are primarily

informational. Clear distinctions are not made between frames designed with a primary intent to inform--through comparative or minimally-biased presentations--and those to persuade--single source presentations, often with strong associative characteristics.

A second issue with regard to reception concerns syndicated and private data bases and personal messages. For interactive systems using common carrier links, issues of privacy would relate directly to the security or integrity of the system. That is, unintended access would result from inadequate security checks--such as passwords or other user identification devices--within the system. The issue for teletext systems is hypothetical, to the best of our knowledge. While we know of no intended "round robin" transmission of private data embedded within public data or grouped with other batches of private data, the technology could be extended to provide this service. Using personally controlled encryption parameters, a system could transmit to all receivers coded data or messages that could presumably be unscrambled only by the intended individual's terminal; such technology has been used for broadcast pay-TV systems. Should this approach emerge, it should be closely scrutinized to insure that it provides adequate protection of privacy.

Issues pertaining to upstream transmissions are of several kinds. Choices of frames viewed could be sensitive. Records of specific frames selected in current videotex systems are not kept by the controlling computer; aggregate totals of

charges incurred are kept, instead. However, additional software could be added to systems implemented in this country, consistent with the expectations of U.S. consumers for itemized bills. The policy or position of corporations who may implement videotex-teletext services in this country is not clear at this time and cannot be predicted.

At first glance, teletext systems--by virtue of their one-way structure--would seem to preclude concern for aggregated records. However, in the WETA pilot study of Telidon, the terminal will be equipped with a meter to record individual responses to aid in the evaluation of the trial. Should teletext systems decide to develop billing policies that include itemizations, such devices could be installed in the home or office and "read" periodically, analogous to a postage meter. If this were done, privacy of records would be an issue.

Another type of sensitive information that could be transmitted upstream and that might raise issues of privacy is credit card information. If Prestel is representative, a high proportion of Information Providers may be commercial, offering buying services to viewers through message frames. Those frames can include lines for entering credit card numbers so that merchandise may be mailed directly to the viewer; but some systems can include credit and mailing information in the viewer's computer profile. In turn, they can add the information when the message frame is "sent" to the Information Provider. Privacy issues may reside both with the Information Providers' use of this information and with the security of such information

within the system, for systems incorporating these features. Voluntary guidelines for handling credit card information have been an item of concern for the Prestel Information Providers Association; the firmness and uniformity of application are not clear at this point.

Once videotex information enters the upstream transmission system, issues of privacy are similar to those issues for common carriers or for interactive cable systems. For systems using the telephone system, there are no new issues raised by this technology. For systems that might be developed that use interactive cable, the issue of privacy would be the generic issue of extending the protection afforded common carriers to interactive cable systems. Hence, no new issues are apparent, other than exposure below the last node, pointed out in the Qube system analysis, should that cable system design be employed.

Within the head-end computer, issues of privacy are primarily issues of security. Since these systems are not fully implemented in this country, policies for direct physical access and for remote access to the system have not been developed. The nature of the problem is made clear when one realizes, for example, that the Prestel Information Retrieval Computers are designed to function without on-site operators. Thus, there may be open issues of security that should be considered.

The next question that must be asked, however, is the nature of the information that could, conceivably, be vulnerable

within the head-end computer. The vulnerability of frame selection records is directly related to whether that information is recorded in the system. More problematic are other "content" services that are a part of some extant and some proposed systems. Information that might be considered private, discussed above with regard to the receiver, includes credit card information and personal messages. Procedures and checks should, of course, be developed to protect these from the intentional eavesdropper.

A more problematic use of information that may be sensitive is that by the Information Provider. A commercial corporation or other Information Provider can receive messages--such as order frames--that are stored in the information retrieval computer. Routinely, the Information Provider collects these and fills the orders. Since these records exist in a machine-readable form, they could be aggregated over time within the information retrieval computer or transferred over a data link to the Information Provider's own computers and aggregated there. The aggregate could be interpreted by a single Information Provider to develop a psychographic profile of the viewer's buying habits or, conceivably, such information could be shared among a number of Information Providers for greater analytic precision and commercial or other use. Currently, we know of no mechanism to control unnecessary use of information by an Information Provider; the only discussion of guidelines we have encountered in this area is for credit card information.

Appendix III. C. GENERAL PURPOSE COMPUTER SYSTEMS

The third type of interactive home media is the system offering general computer retrieval and other services to the consumer. This type of system employs standard data processing links and standard computer terminals, rather than converted TV sets, as output devices. As a result, the nature and form of the information provided the user are different from that provided by the other systems described in this report. Information is not necessarily page-oriented, although some specific requests are printed or displayed in a page format; rather, information is more likley to be displayed as a continuous succession of lines. Information is primarily text textual and character-oriented; no graphic output is currently provided. However, a much larger range of interaction is possible.

An Example: The Source

The primary instance of this category is The Source, located in McLean, Virginia. In developing this description, we reviewed the published literature, examined company descriptive materials, and talked with Dr. Michael Hills, Vice President-Director, Technology.

Among The Source's services are these:

- personal finance systems--in which the user can enter financial records, retain, and modify them;
- electronic mail--in which free format correspondence of considerable length can be composed, transmitted to another user, and return acknowledgement requested;
- educational programs--in which two-way instruction is offered on a variety of subjects for students from pre-school to post-graduate;

- general computer utilities--providing retrieval, mathematical modelling, and statistical analysis; and
- general batch and time-sharing services--in which users may develop, store, and use their own software in several popular computer languages.

Additional offerings include:

- news wire services;
- market quotation services;
- entertainment services; and
- games.

While The Source is likely to appeal to the more educated, professional individual, its versatility and power make its long-term aggregate use potentially as high as more popularly-oriented systems.

1. System Overview: THE SOURCE

The Source can be characterized as a system that provides the general consumer with a range of services through a general purpose computer system. The system in many respects is similar to those of computer centers on academic campuses, in government agencies, or in industry, but with a number of non-technical consumer services added. It relies on established computer technology rather than specially developed new technologies, as with interactive cable systems and videotex-teletext systems.

The head-end computers are currently a pair of large mini-computers, but The Source states they expect to expand soon to large IBM mainframe machines. The system appears to run under a conventional operating system (they regard this information as proprietary) and offers the conventional statistical packages, programming languages, and file/editor systems that are expected of any general purpose system. The distinguishing aspect of this system, however, is the specialized software (computer programs) that provide the general non-technical consumer services outlined above.

As with most general systems, the primary mode of access is through a remote typewriter terminal linked to the system via telephone lines. The system does not rely on the TV set as a display device but, instead, requires that the consumer obtain a computer terminal. Such devices currently start at $700-$800; however, some personal computers can be used as terminals and can, hence, be used to access The Source. The

costs for the terminal, then, are competitive with, and in some instances, less than the conversion units required to adapt the TV set to receive videotex-teletext services.

Communications between the terminal and the head-end computer is provided by the telephone. The terminal uses a device, called a modem ($100-$200), that translates typed characters into audible signals that are transmitted and, in turn, translate signals received into characters to be displayed on the terminal. Consumers in the Washington area may call The Source by simply dialing their telephone. Consumers elsewhere may do the same, but must pay long distance toll charges. Alternatively, however, consumers in most metropolitan areas can call a local number in their area and enter one of several commercial data transmission systems with whom The Source has contractual arrangements. Under these arrangements, consumers pay only the normal charges computed on the basis of the length of time they use The Source and do not pay any separate or additional communication costs.

2. Technical Description: THE SOURCE

Head-End Computer

The current two head-end computers are Prime 750's; they are expected to grow to four in the near future. These are large 16-bit minicomputers each with 300 megabytes of disk storage and each capable of supporting some 100 users. Within the year, The Source plans to move to large IBM 3033 processors, each of which is expected to support approximately 1000 simultaneous users. (See Glossary, Appendix VI.)

Software for the system was developed by The Source and the details of its design are regarded as proprietary. In general, the user, when connected to the system, enters under a general monitor that provides basic editing and file support; this approach is typical of most large academic, corporate, and government systems. Users then select the particular data base or service desired and the monitor routes inquiries and instructions to that subsystem. Most of these services are provided by a half-dozen or so generic software systems that, in turn, access different collections of data. For example, the same programs might be used to support inquiries to all of the various market data bases. As is also typical with general multi-purpose computer systems, users have access to files that may contain personal data or software they have developed. The latter may then be executed to probe various collections of data or to perform analyses. Thus, individuals may use the system at a general consumer level, supported by software designed to require the least technical understanding

of the system, or they may use the system at a technical level as with conventional computer centers.

Transmission

The link between users and The Source is handled entirely through the phone system and public high-speed data links. Local users may call The Source directly using a standard telephone. Subscribers in distant metropolitan areas use one of the commercial packet-switching systems, such as Telenet. This is done by calling a local telephone number and identifying self and The Source; in turn, one is connected to The Source through a high-speed, shared data link. All charges for this connection are included in the single hourly rate charged by The Source ($4.25/hour non-prime; $15.00/hour business hours). Users not living in an area served by one of the packet-switching services must pay toll costs.

Terminal

Acceptable terminals are virtually any standard data processing terminal and most home micro-computers (with a special phone connector or modem). The terminal is the sole responsibility of the subscriber. Currently, the cheapest cathode ray tube terminal sells for approximately $700 and the necessary phone connection (300 baud modem) for $100-$200.

It is interesting to note the comparative economics of the conventional data processing terminal versus the converted TV set used by videotex-teletext systems. The data processing terminal typically displays 80, instead of 40, characters per row and, hence, has twice the display capacity as the TV set.

At $800, a minimum terminal configuration is cheaper than the specially developed videotex units being sold (typically, approximately $1,500). Even some of the conversion systems cost as much as the data processing terminal. While cost factors are often mentioned by those advocating TV-oriented media, familiarity, acceptance, and other social or cultural factors associated with TV may actually be more significant in determining near-term development and growth in the consumer computer-supplied information industry.

3. Privacy and Security: THE SOURCE

The Source assumes responsibility for both the system and the information; consequently, it retains the right to control content that may be regarded as offensive by some individuals. Data is provided to The Source on a contract basis by Information Providers, under several types of agreements. In some instances, The Source contracts for data to be provided to it on an exclusive basis; in other instances, such as the UPI wire service, it contracts along with many others to receive the data. In the former instance, The Source retains the right to return for modification data unacceptable; in the latter, The Source retains the right to delete material it believes may be offensive. However, while retaining the ultimate right to reject, The Source is uncomfortable with the role of censor. One of the more troublesome areas, we are told, is the posting of notices of questionable taste in a system approximating a public bulletin board. The Source says it is being vigilant; but it has not provided a systematic answer to this problem.

A wide variety of information is generated at the terminal that might be regarded as private. Personal finance data, messages, and small business accounting information are some of the more obvious instances. Since word processing services are offered, a number of other kinds of written documents are stored in The Source system and may be regarded as private. Again, various purchasing services are offered, ranging from booking travel reservations to ordering merchandise by mail.

Appendix IV.

NEXT STEPS--RECOMMENDATIONS

Appendix IV. NEXT STEPS--RECOMMENDATIONS

In this report, Collingwood Associates:

- established a general framework for understanding the privacy issues associated with interactive home media systems; and
- recommended the next research steps required to refine these findings, set goals, and select strategies for action.

The framework established encompasses three types of interactive home media, each offering a different degree of consumer interaction. It identifies four major privacy issues raised by these systems: intrusion, interception, misuse of information, and aggregation by household.

To refine this framework, we urge that the Federal Trade Commission immediately take these six steps:

1. Undertake or commission a full-scale examination of federal, state, and local statutes pertaining to privacy that do or can relate to the interactive home media field. This study should include a survey of all federal agencies for their current activities and plans specifically touching upon the question of privacy. The product of such a study should include a framework of privacy interests for policy makers.

2. Undertake or commission a study of the economic structure of the interactive home media industry, especially as it bears on privacy and other consumer-related concerns.

3. Determine the level of privacy protection needed and feasible.

4. Encourage forms of industry self-regulation in this area.

Personal files for which one wishes to control access are protected by user-supplied passwords and account numbers. As an extra precaution, The Source advocates use of passwords that include "escape characters" that do not actually print or show on the terminal but are recognized by the computer. The Source's protection against eavesdropping seems reasonable, although two possible, but extreme, possibilities can be foreseen. As a service, The Source provides consultants who can help users having difficulty with the system. In some instances, the consultant may be asked to look at the contents of a file. To do so on a password-protected file requires the user to supply the password; since the user initiates all such consultations and since the user may change the password, exposure here seems within the power of the user to control. The second exposure is more unusual. The computer must retain copies of all passwords to verify each specific password at time of access. Since the system supports user-developed software, there is the possibility that some individual may take the extreme step of writing an "illegal" program that attempts to uncover the list of passwords. (Readers familiar with academic computer centers will undoubtedly recall the exceptional undergraduate who comes along every five years or so and succeeds in "breaking the bank".) The Source states that is has placed "traps" in its software to detect such unwarranted access, but the firm refuses to discuss these precautions on proprietary grounds.

Appendix V.

BIBLIOGRAPHY

Appendix V. BIBLIOGRAPHY

This bibliography reflects those articles found useful in the development of this report. The listing is in no way meant to be definitive.

The bibliography is arranged as follows:

5. Provide consumer education services, including printed material, about these new media.

6. Work on an inter-governmental plan to develop strategies for action, where government action is warranted.

Elton, Martin. "Interactive Telecommunications." 3 (2) Telecommunications Policy (June 1979): 153.

Freid, Charles. "Privacy." 77 (3) Yale Law J (January 1968): 475.

Gavison, Ruth. "Privacy and Its Legal Protection." Unpublished D. Phil. thesis on file in Oxford, Harvard Law School, and Yale Law School libraries, 1975.

Gavison, Ruth. "Privacy and the Limits of Law." 89 Yale Law J (1980): 421.

Gerety, T. "Redefining Privacy." 12 (2) Harvard C.R. L Rev (Spring 1977): 233.

Goldman, Ronald J. "Demand for Telecommunications Services in the Home." 4 (1) Telecommunications Policy (March 1980): 25-30.

Greenawalt, Kent. Legal Protection of Privacy. Washington, D. C.: Office of Telecommunications Policy, 1975.

Greenawalt, Kent. "New York's Right of Privacy: The Need for Change.: 42 Brooklyn L Rev (1975): 159.

Gregurs, J.F. "Informational Privacy and the Private Sector." 11 Creighton L Rev (October 1977): 312-51.

Karuse, H.D. and P. Marcus. "Privacy." 26 Am J Comp L (1978): 377-92.

Kronman. "The Privacy Exemption to the Freedom of Information Act." Journal of Legal Studies (1980).

Larsen, Kent (ed.). Privacy, A Public Concern: A Resource Document. Washington, D. C.: U.S. Government Printing Office, August 1975.

Metelski, J. "Achieving Communications Privacy through Revision of the Eavesdropping Laws." 30 (2) Federal Communications L J (Summer 1978): 135-47.

Michael. "On Coping with Complexity: Planning and Politics." 97 Daedalus (1968): 1179.

Miller, A.S. "Privacy and the Modern Corporate State: A Speculative Essay." 25 Ad L Rev (Summer 1973): 231-67.

Mossman, K. "New Dimension of Privacy." 61 ABA Journal (July 1975): 829-33.

O'Brien, D.M. "Privacy and the Right of Access: Purposes and Paradoxes of Information Control." 30 Administrative L Rev (Winter 1978): 45-92.

I.

PRIVACY: DEFINITIONS

Baer, Walter S. "Controlling Unwanted Communications to the Home." 2(3) Telecommunications Policy (September 1978): 218-228.

Ballard, David P. "Privacy and Direct Mail Advertising." 47 Fordham L Rev (March 1979): 495-526.

Barron, J.H. "Warren and Brandeis. The Right to Privacy: Harvard L Rev (1890): Demystifying a Landmark Citation." 13 Suffolk Univ L Rev (Summer 1979): 875-922.

Bazelon. "Probing Privacy." 12 Gonz L Rev (1977): 587, 592.

Bloustein, Edward. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." 34 NYU L Rev (1964): 962.

Brant, J. "General Introduction to Privacy." 61 Mass L Q (Spring 1976): 10-18.

Coates, J. "Aspects of Innovation--Public Policy Issues in the Telecommunications Development." 1 Telecommunications Policy (1977): 196-206.

Comment. "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision." Calif L Rev (December 1976): 1447-83.

Computer and Business Equipment Manufacturers Association. Fifth State Legislation Status Report: 1980. Washington, D. C.: CBEMA, 1980.

Computer and Business Equipment Manufacturers Association. 1980 Privacy and Security Bibliography. Washington, D. C.: CBEMA, 1980.

"Constitutional Right of Privacy: An Examination." 69 Northwestern Univ L Rev (May-June 1974): 263-301.

Cox. "A Walk Through Sec. 552 of the Administrative Procedures Act: The Freedom of Information Act; the Privacy Act; and the Government in the Sunshine Act." 46 Univ of Cin L Rev (1978): 969.

Dickler. "The Right of Privacy." 70 US Rev (1936): 435.

Epstein. "Privacy, Property Rights, and Misrepresentation." 12 Georgia L Rev (1978): 455.

Eichbaum, J.A. "Towards an Autonomy Based Theory of Constitutional Privacy: Beyond the Ideology of Familial Privacy." 14 Harvard CR L Rev (Summer 1979): 361-84.

Swan, P.N. "Privacy and Record Keeping: Remedies for the Misuses of Accurate Information Systems." 54 NC L Rev (April 1976): 585-640.

"Symposium: Openness in Government--A New Era." 34 Federal Bar Journal (Fall 1975): 279-366.

Towe, T.E. "Growing Awareness of Privacy in America." 37 Montana L Rev (Winter 1976): 39-89.

"Triangulating the Limits of the Tort of Invasion of Privacy: The Development of the Remedy." 3 Hastings Const L Q (Spring 1976): 543-98.

"United States v. Miller (96 Sup Ct 1619): Without a Right to Information Privacy, Who Will Watch the Watchers?" 10 John Marshall J (Spring 1977): 629-50.

Warren, Samuel and Brandeis, Louis. "The Right to Privacy." 4 Harvard L Rev (1890): 193.

Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1968.

Palmer, G. "Privacy and the Law." NZ Law Journal (November 1975): 747-56.

Parker, R.B. "Definition of Privacy." 27 Rutgers L Rev (Winter 1974): 275-96.

Pennock, R. and Chapman, J. "Privacy." NOMOS, XIII (Yearbook of the American Society for Political and Legal Philosophy, 1971).

Posner, Richard. "Privacy, Secrecy, and Reputation." 1 Buffalo L Rev (1979): 1.

Posner, Richard. "The Right to Privacy." 12 Georgia L Rev (1978): 393.

"Privacy and Economics: The Right of Privacy." 12 Birmingham Georgia L Rev (Spring 1978): 393-551.

"Privacy Issues in Data, Voice, and Video Communications." Seminar: Telecommunications Policy Planning and Research at MIT, May 22, 1974.

Privacy Protection Study Commission. Personal Privacy in an Information Society. Washington, D. C.: U.S. Government Printing Office, July 1977.

"Privacy." Special Issue. 31 Law and Contemporary Problems (Spring 1966).

"Privacy: The Search for a Standard.: 11 Wake Forest L Rev (December 1975): 659-89.

"Privacy's Parasite: A Symposium." 11 Trial (January-February 1975): 12.

Prosser, William. "Privacy." 48 Calif L Rev (1960): 383.

Prosser, William. The Law of Torts, 4th Edition (1971): 802-804.

Rosenburg, Jerry M. The Death of Privacy. New York: Random House, 1969.

Silver, I. "Future of Constitutional Privacy." 21 St Louis U L J (1977): 211-80.

Smith, Robert Ellis. Compilation of State and Federal Privacy Laws, 1978-1979. Washington, D. C.: Privacy Journal, 1978.

Smith, Robert Ellis. Privacy: How to Protect What's Left of It. New York: Anchor Press/Doubleday, 1979.

Storey, J. Infringement of Privacy and Its Remedies. 47 Aust L J (Summer 1973): 498-515.

Hoffman, L. Security and Privacy in Computer Systems. Los Angeles: Melville Publishing Company, 1973.

Holmes, Grace. Law of Computers. Ann Arbor, MI: Institute of Continuing Legal Education, 1971. (Includes: Loevinger, Lee, "Communications Regulation," pp. 121-131.)

"Interdependence of Communications and Data Processing: An Alternative Proposal for the Second Computer Inquiry." Northwestern U L Rev (May-June 1978): 307-58.

Katzen, Harry. Computer Data Security. New York: V. Nostrand Reinhold Co., 1973.

Little, Arthur, Inc. The Consequences of Electronic Funds Transfer. Cambridge: Arthur D. Little, Inc., June 1975.

Linowes, D.F. "Must Personal Privacy Die in the Computer Age?" 65 ABA Journal (August 1979): 1180-4.

Martin, James. The Computerized Society. Englewood Cliff, NJ: Prentice-Hall, 1970.

Martin, James. Security, Accuracy, and Privacy in Computers. Englewood Cliffs, NJ: Prentice-Hall, 1973.

Miller, Arthur R. Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor, MI: The University of Michigan Press, 1971.

Prives, Daniel. The Explosion of State Laws on Electronic Transfer Systems: Its Significance for Financial Institutions, Non-Financial Institutions, and Consumers. Cambridge: Harvard University Program on Information Technologies and Public Policy, 1976.

"Public Access to Government Held Computerized Information." 68 Northwestern U L Rev (May-June 1973): 433-62.

Ralston, Anthony (ed.) Encyclopedia of Computer Science. New York: Petrocelli/Charter, 1976.

"Report of the Subcommittee of the Law Revision Commission on Computer Data Banks and Privacy." 6 NZ U L Rev (October 1974): 190-4.

Ruder, Brian. An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse. Washington, D. C.: U.S. Government Printing Office, U.S. National Bureau of Standards.

Search Group, Inc. Standards for Security and Privacy of Criminal Justice. Sacramento: Search Group, Inc., January 1979.

II.

PRIVACY AND SECURITY: COMPUTER SYSTEMS

Baran, Paul. "On Distributed Communications. IX: Security, Secrecy, and Tamper-Free Considerations." Security and Privacy in Computer Systems, ed. L. Hoffman. Los Angeles: Melville Publishing Company, 1973.

Berman, P.J. and Oettinger, A.G. "Changing Functions and Facilities: The Politics of Information Resources." 28 Federal Communications Bar Journal (1975): 227-73.

Blue, Richard B., Sr. and Gerald E. Short. Computer System Security Technology and Operational Experience. Redondo Beach, CA: TRW Systems, Inc., March 1974.

Bushkin, Arthur. The Security Implications of Privacy. McLean, VA: System Development Corp., June 1975.

Canadian Government, Departments of Communications and Justice. Privacy and Computers. Ottowa: Crown Copyright, n.d.

Carroll, J.M. and P.M. McLellen. "Fast 'Infinite-Key' Privacy Transformation for Resource Sharing Systems." Security and Privacy in Computer Systems, ed. L. Hoffman. Los Angeles: Melville Publishing Company, 1973.

"Computer or Communications? Allocation of Functions and the Role of the FCC." 27 Federal Communications Bar Journal (1974): 161-230.

Computer Security Research Group. Computer Security Handbook. New York: MacMillan Publishing Company, 1973.

"Computers, Privacy Create Social Issues." 22 Infosystems (November 1975): 18.

Corbett, J. "Computers and the Protection of Privacy." 126 New L Journal (June 3, 1976): 556-9.

Cutler, C. "Government Regulation of the Computer Industry--Computer Communication and Industry, etc." Washington Univ L Quarterly (1977): 469-97.

Davis, R.M. "Technologist's View of Privacy and Security in Automated Information Systems." 4 Rutgers Journal Computers and Law (1975): 264-82.

Goldstein and Holen. "Personal Privacy v. the Corporate Computer." 53 Harvard Bus Rev (1975): 62.

Halls, C.C. "Raiding the Databanks: A Developing Problem for Technologists and Lawyers." 6 Journal of Contemporary Law (Spring 1979): 245-66.

U.S. National Bureau of Standards and MITRE Corporation. The Privacy Mandate: Planning for Action. Washington, D. C.: NBS, August 1975. (Workshop summary.)

Ware, Willis. "Handling Personal Data." Datamation (October 1977).

Ware, Willis. Testimony before the National Commission on Electronic Funds Transfer. Santa Monica: Rand Corporation, December 1976.

Ware, Willis. Testimony before the Subcommittee on Communication Hearings: Impact of Telecommunications Technology on the Right to Privacy. Santa Monica, CA: Rand Corporation, August 1977.

Weisner, Jerome. Testimony before the U.S. House Government Operations Committee. Hearings on The Computer and the Invasion of Privacy, July 26-28, 1966.

Wessel, M.R. "Computers/Privacy--A Lawyer's View." Freedom's Edge. Addison-Wesley, 1975.

Westin, A. Databanks in a Free Society: Computers, Record-Keeping, and Privacy. New York: Quadrangle Books, 1972. (National Academy of Sciences project.)

Westin, A. Information Technology in a Democracy. 1977.

Westin, A. "Science, Privacy, and Freedom Issues and Proposals for the 1970's." 66 Columbia L Rev: 1003-1050.

"Symposium: Computers, Data Banks, and Individual Privacy." 53 Minnesota L Rev (1968): 211.

Turn, Rein. Privacy and Security in Personal Information. Santa Monica, CA: The Rand Corporation, March 1974. (NSF funded.)

U.S. Congress. Information Policy: Public Laws from the 95th Congress. Washington, D. C.: Government Printing Office, 1979.

U.S. Congress, House Government Operations Committee. Hearings, The Computer and Invasion of Privacy. 90th Congress, 2d Session, March 12-14, 1968.

U.S. General Accounting Office. Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment. Washington, D. C.: GAO, 1978.

U.S. General Accounting Office. Improved Planning: A Must Before a Department-Wide Automatic Data Processing System Is Acquired for the Department of Agriculture. Washington, D. C.: GAO, June 3, 1975.

U.S. General Accounting Office. Safeguarding Taxpayer Information: An Evaluation for the Proposed Computerized Tax Administration System. Washington, D. C.: GAO, January 17, 1977.

U.S. General Accounting Office. Vulnerabilities of Telecommunications Systems to Unauthorized Use. Washington, D. C.: GAO, 1977.

U.S. Hanscom Air Force Base, Electronic System Division. Government Applications: Computer Security Developments: Summary. Hanscom AF Base, 1974.

U.S. Department of Health, Education, and Welfare. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, D. C.: Government Printing Office, 1973. (Also published as "Records, Computers and the Rights of Citizens," Datamation, September 1973.)

U.S. National Bureau of Standards. "Approaches to Privacy and Security in Computer Systems." Proceedings of a conference held at the National Bureau of Standards, Gaithersburg, MD, March 4-5, 1974.

U.S. National Bureau of Standards. "Computer Security and the Data Encryption Standard." Proceedings of the Conference on Computer Security and the Data Encryption Standard. Washington, D. C.: U.S. Government Printing Office, 1978.

U.S. National Bureau of Standards. Institute for Computer Sciences and Technology. Computer Security Guidelines for Implementing the Privacy Act of 1974. Washington, D. C.: NBS, May 30, 1975.

IV.

CABLE

Albert, James A. "The Federal and Local Regulation of Cable Television." 48 University of Colorado L Rev (1977): 501.

Babe, Robert E. "Public and Private Regulation of Cable Television: A Case Study of Technological Change and Relative Power." 17 Canadian Public Administration (1974): 187.

Baldwin, Thomas F. and others. "Public Policy in Two-Way Cable." 3(2) Telecommunications Policy (June 1979): 126-133.

Cabinet Committee on Cable Communications. Report to the President. Washington, D. C.: Office of Telecommunications Policy, 1974.

CATV Today: Discussion of Current Events. Washington, D. C.: Georgetown School for Summer and Continuing Education, 1975.

Ciporen, Helaine. "Cable Systems: Meeting a Growing Need." 2(1) Info for Your Future (Winter 1980): 19.

Goldman, Ronald J. "Demand for Telecommunications Services in the Home." Paper presented at the Annual Meeting of the International Communications Association, Philadelphia, PA, May 1-5, 1979.

Johnson, Leland. The Future of Cable Television: Some Problems of Federal Regulation. Santa Monica, CA: Rand Corporation, January 1970.

Johnson-Hall, Martha. Report on Qube. Washington, D. C.: Department of Commerce, National Telecommunications and Information Administration, n.d. (1980).

Kay, Peg. "Policy Issues of Interactive Cable Television." 28 Journal of Communications (1978): 202-208.

Kay, Peg. Social Services and Cable TV. Washington, D. C.: Cable Television Information Center, July 1976.

Mason, William and Sidney Polk (Mitre Corporation). "Revolutionizing Home Communications: New Techniques for Using Computers with Cable Television." Paper presented at the IEEE Intercon, March 20-23, 1978.

New York State Commission on Cable Television. Cable Communications in New York State: An Agenda for Government Involvement. August 1979.

Oppenheim, Jerrold. "The Coaxial Wiretap: Privacy and the Cable." 2 Yale Review of Law and Social Action (1972): 282.

"Privacy of Two Way CATV Systems." 5 C L S R (1976): 740.

III.

INTERACTIVE MEDIA (GENERAL)

Baran, Paul. Potential Market Demand for Two Way Information Services to the Home: 1970-1990. Menlo Park, CA: Institute for the Future, December 1971.

Coates, Joseph. "Aspects of Innovation-Public Policy Issues in Telecommunications Development." 1(3) Telecommunications Policy (June 3, 1977): 196-206.

Elton, Martin. "Interactive Telecommunications." 3(2) Telecommunications Policy (June 1979): 153.

Fay, Tim. "Wired Nation Decoded." Public Telecommunications (November 1979): 1.

Goldman, Ronald J. "Demand for Telecommunications Services in the Home." 4(1) Telecommunications Policy (March 1980): 25-30.

Grew, Suzanne. World's First Trials of New Information Systems. Ontario Educational Communications Authority, January 31, 1980.

Johansen, Robert and others. "Issues and Insights for the USA." 4(1) Telecommunications Policy (March 1980): 31-41.

Mahony, S., N. DeMartino, and R. Stengel. Keeping Pace with the New Television. New York: Carnegie Corporation of New York, 1980.

Ministry of Posts and Telecommunications. Report on Present State of Communications, 1978. Japan: The Look Japan Ltd., 1978.

Ministry of Posts and Telecommunications. Report on the Present State of Communications in Japan, 1979. Japan: The Look Japan Ltd., 1979.

Noll, Michael A. "Service and System Implications." 4(1) Telecommunications Policy (March 1980): 17-24.

U.S. Senate Commerce Committee, Subcommittee on Communications. Oversight of Rural Telecommunications. 95th Congress, 1st Session. April 6, 1977.

V.

TELETEXT AND VIEWDATA

Bell, Daniel. "Teletext and Technology." Encounter (June 1977): 9-29.

Brown, H.G. and others. A General Description of Telidon: A Canadian Proposal for Videotex Systems. Ottowa: Department of Communications, Communications Research Centre, December 1978.

Butler, Cox and Partners, Ltd. Videotex and Its Potential Impact in Europe. 3 volumes. London: Link in association with Butler Cox and Partners, Ltd., 1978.

Cioni, Maria L. "The OECA and Telidon." TV Ontario, July 25, 1979.

Clark, Richard. "Videotex: An Overview of Electronic Information Services." Computer Communications (April 1979): 51-55.

Criner, Kathleen. U.S. Videotex Activities and Policy Concerns. 4 (1) Telecommunications Policy (March 1980): 3-8.

Fedida, S. "Optimizing View Data." Wireless World (June 1978): 75-77.

Fedida, S. "Viewdata: The Post Office's Textual Information and Communications System--Background and Introduction." Wireless World (February 1977): 32-36.

Fedida, S. "Viewdata--2 Applications of the System." Wireless World (March 1977): 52-54.

Fedida, S. "The Viewdata Computer." Wireless World (April 1978): 44-48.

Fedida, S. "Viewdata--3 Operation of the System: Terminals and Codes." Wireless World (April 1977): 65-69.

Fedida, S. "The Viewdata Computer--2." Wireless World (May 1978): 73-76.

Fedida, Sam and Malik, Rex. The Viewdata Revolution. New York: John Wiley & Sons, 1979.

Flaherty, Joseph. "Teletext: The Magazine of the Future." 2 (1) Info for Your Future (Winter 1980): 5.

Grundfest, Joseph and Brotman, Stuart N. Teletext and Viewdata: The Issues of Policy, Service, and Technology. Aspen, CO: Aspen Institute Program on Communications and Society, 1979.

"QUBE-Interaction on the Cable: How Columbus Residents Can Register Their Opinions and Shop by TV." Educational and Industrial Television (April 1979): 45.

Sloan Commission on Cable Communications. On the Cable: The Television of Abundance. New York: McGraw-Hill, 1971.

Smith, Ernest and others. System Control Facilities: Head-Ends and Central Processors: A Survey of Technical Requirements for Broadband Cable Teleservices. Vol. 4. Washington, D. C.: Department of Commerce, Office of Telecommunications, 1973.

"Special Topic: Communications Technology and the Delivery of Legal and Government Services." 55 Univ of Detroit Journal of Urban Law (Spring 1978): 649-781.

Tate, Charles. Cable TV in the Cities: Community Control, Public Access, and Minority Ownership. Washington, D. C.: Urban Institute, 1971.

"Toward Community Ownership of Cable TV." 83 Yale L J (1974): 708, 1709-10.

U.S. Congress, House Interstate and Foreign Commerce, Communications Subcommittee, Staff Report. Cable Television: Promise vs. Regulatory Performance, January 1976.

U.S. Congress, House Interstate and Foreign Commerce, Communications Subcommittee. Hearings, Cable TV Regulation Oversight: The Role of Congress in Regulating Cable Television and the Potential for New Technologies in the Communications System. Part 2, 1976.

U.S. Senate Commerce Committee, Communications Subcommittee. Karen Posner (staff). "Options for Cable Television Regulation," in Option Papers. Washington, D. C.: Government Printing Office, May 1977.

U.S. National Science Foundation. "Interactive Cable TV--Three Studies." 3(3) Telecommunications Policy (September 1979): 245-249.

Vieth, Richard. Talk-Back TV: Two Way Cable Television. Blue Ridge Summit, PA: Tab Books, 1976.

Wicklen, J. "Wired City, USA: The Charms and Danger of Two Way Cable." 243 Atlantic (February 1979): 35-42.

Roizen, Joseph. "The Technology of Teletext and Viewdata." Videotext: The Coming Revolution in Home/Office Information Retrieval, Efrem Sigel, ed. White Plains, NY: Knowledge Industry Publications, Inc., 1980.

Rosch, Gary D. "The Technical Side of Viewdata." 10 Telephony (July 1978): 140.

Scott, David. "Teletext/Viewdata Converts Your TV Set into an Instant Information Service." Popular Science (May 1978): 108-11.

Sifton, John and Wright, David. "Canada: Major Support for Telidon." 7 (3) Intermedia (May 1979): 30-32.

Strangeways, Richard. "Teletext: Hardware Design Approach." Broadcasting Systems and Operation (September 1978): 15-16.

Syrett, John. Telidon and Education. Ontario Educational Communications Authority, July 20, 1979.

Telegen Corporation. "An Introduction to Teletext Systems." Educational and Industrial Television (June 1979).

Teletext and Viewdata. Luton, England: Mackintosh Publications, Ltd., 1977.

Tomita, Tetsuro, "Japan: The Search for a Personal Information Medium." 7 (3) Intermedia (May 1979): 36-38.

Tyler, Michael. "Videotex, Prestel and Teletext: The Economics and Politics of Some Electronic Publishing Media." 3 (1) Telecommunications Policy (March 1979): 37-51.

"Videotex: Words on the TV Screen; Viewdata, Teletext, and the Rest." 7 (3) Intermedia (May 1979): 6-10.

Viewdata and Its Potential Impact in the USA. 2 vols. London: Link in association with Butler Cox and Partners, Ltd., 1978.

"Viewdata: A Review and Bibliography." Online Review (September 1978): 217-224.

Winsbury, Rex. The Electronic Bookstall: Push-Button Publishing on Videotex. London: International Institute of Communications, 1979.

Winsbury, Rex and Lane, Martin. "Prestel Is the First to Start." 7 (3) Intermedia (May 1979): 10-17.

Guinet, Y. "Comparative Study of Broadcast Teletext Systems. Some Advantages of the Application of Packaged-Data Broadcasting to Teletext." EBU Review: Technical Part, No. 165 (October 1977): 242-254.

Guinet, Y. "New Services Offered by a Packaged-Data Broadcasting System." EBU Review: Technical Part, No. 149 (February 1975): 3-10.

Hedger, J. "Telesoftware: Home Computing via Teletext." Wireless World (November 1978): 61-64.

Hill, Donald K. "Communications, Public Interest, and Community Participation." Texas Southern L Rev (December 1970).

"Home Data Banks Turn British On: Prestel." 114 Sci News (July 22, 1978): 54.

Johnson, G.A. and Leduc, N.F. "Vista: A New Interactive Visual System." 1 (1) Info for Your Future (Fall 1979): 11.

Johnson-Hall, Martha. "NTIA to Coordinate Teletext Project." Commerce News (June 6, 1980).

Leduc, Nicole. "Introducing the Vista System." 3 (2) Telecommunications Policy (June 1979): 155.

Lemelschtrich, Noam. Design Analysis of a Home Terminal of Two Way Communication. New York: Center for Policy Research, Inc., February 1972.

Logue, T.J. "Teletext: Towards an Information Utility?" 29 (4) Journal of Communication (Autumn 1979): 58-65.

Loveless, Bill. "The Broadcasting of Teletext." Educational and Industrial Television (June 1979).

"Microprocessor Smartens Teletext." Electronics (September 28, 1978): 74.

Nakahara, Tsuneo and others. "An Optical Fiber Video System." 26 IEEE Transactions on Communications (July 17, 1978): 955-62.

O'Conner, Robert. "Teletext Is Coming: A Symposium." Education and Industrial Television (June 1979): 33.

Pye, Roger. "The Birth of a Videotex Industry." 7 (3) Intermedia (May 1979): 41-47.

Roizen, Joseph. "The Current State of International Teletext Technology." TV Communications (July 1978): 42-43.

Roizen, Joseph. "The French ANTIOPE System." Educational and Industrial Television (June 1979): 36.

Appendix VI.

GLOSSARY

Appendix VI. GLOSSARY

BAUD - a measure of the transmission rate of data over a telephone line or other channel. The baud rate divided by 10 will normally be the rate of transmission in characters per second (e.g., 1200 baud is 120 characters per second).

BIT - the smallest logical unit of information; a bit can assume one of two values, usually represented as "0" and "1". Bits are aggregated into sequences, normally six or eight, to form units called bytes.

BRIDGE GATE CONTROLLER - a device in an interactive TV cable transmission system that permits messages to be sent in both directions (e.g., upstream as well as downstream).

BYTE - the primary unit used to describe storage capacity of a computer. Normally consisting of a group of six or eight bits, one byte is used to represent and store one character (e.g., an "A" or a "$") of information.

COMPUTER TYPES

- MAINFRAME - large general purpose machines typically offering a wide variety of both batch and interactive services to numerous (several hundred to a thousand) users simultaneously. Processor is 32 bits or larger; cost: typically several millions of dollars.

- MINI-COMPUTER - medium sized machines that typically offer one or several types of services to from a dozen to approximately 100 users. Processor is usually 16 bits; cost: typically several hundreds of thousands of dollars.

- MICRO-COMPUTER - small systems that range from those providing single service to a single user (personal computer) to several services to approximately a dozen users. Processor is usually eight bits; cost: $500 to approximately $20,000.

CRT - a common low cost type of computer terminal using a typewriter keyboard and a cathode ray tube display screen.

DISK - an external storage device used to store large quantities of information (up to approximately 500 million bytes per unit) in a form where any portion of it can be retrieved by the computer in a few thousandths of a second. The device resembles a large phonograph record with a continuous ferro-magnetic surface and a movable re/write head that can jump to fixed locations ("tracks") to record or read data in random order.