Federal Communications Commission
Office of Plans and Policy
1919 M Street, N.W.
Washington, D.C. 20554

A Working Paper on:

# 5 Economics and Telecommunications Privacy: A Framework for Analysis

December 1980

---

By: James A. Brown, Jr.
Kenneth Gordon

The FCC Office of Plans and Policy's Working Paper Series presents staff analysis and research in various stages. These papers are intended to stimulate discussion and critical comment within the FCC, as well as outside the agency, on issues in telecommunications policy. Titles may include preliminary work and progress reports, as well as completed research. The analyses and conclusions in the Working Paper Series are those of the authors and do not necessarily reflect the views of other members of the Office of Plans and Policy, other Commission staff, or the Commission itself. Given the preliminary character of some titles, it is advisable to check with authors before quoting or referencing these Working Papers in other publications.

Copies may be purchased from the International Transcription Service, FCC, 1919 M Street, N.W., Washington, D.C., (202) 296-7322. Copies are also available from The National Technical Information Service, Springfield, VA 22161 (703/487-4650). The inside back cover contains a list of previous titles.

For information on the Series, contact the Office of Plans and Policy, Federal Communications Commission, Room 838, 1919 M Street, N.W., Washington, DC 20554 (202/653-5940).

December 1980

# Economics and Telecommunications Privacy: A Framework for Analysis*

James A. Brown, Jr.
Kenneth Gordon

Office of Plans and Policy
Federal Communications Commission
Washington, D.C. 20554

* The opinions expressed in this paper are the authors'. They do not necessarily reflect policies or views of the Federal Communications Commission or any other organization or individual. We are particularly indebted to Doug Webbink and Nina Cornell for many helpful suggestions.

Table of Contents

ABSTRACT
ECONOMICS and TELECOMMUNICATIONS PRIVACY:
A FRAMEWORK for ANALYSIS

This paper is an overview of privacy, particularly as related to telecommunications policy, from an economic perspective. The general framework is the economics of information. Information about people and organizations is a valuable economic input to decision making. Moreover, privacy also may be analyzed as an economic good insofar as resources devoted to the production of privacy must be taken from elsewhere. That is, more privacy usually means less of some other good or service.

Because the value of information often depends on its security and because information about both individuals and organizations can be used in inimical ways, society has valid concerns about invasions of privacy. Many fear rapid change in communications and data processing are eroding privacy in ways unimaginable only a few years ago. One result has been a series of legislative proposals to regulate information gathering, use, and dissemination.

Seclusion, personal privacy, business or commercial privacy, and theft of telecommunications signals each involve different privacy problems. Seclusion (the right to be let alone) is valued for its own sake, yet it may conflict with desires of others to communicate with an individual. Personal information privacy may be threatened especially by electronic data storage and transmission and by availability of detailed customer records for services like interactive cable TV. But information privacy is neither simple nor straightforward. Privacy for individuals may mean less information for others who deal with them. So it may reduce economic output. Thus, any legislation affecting the flow of personal information may have far-reaching, and not always desirable, effects on productivity and income distribution. Somewhat different, and perhaps less emotional, concerns apply to commercial and industrial privacy. In particular, firms often legitimately need confidentiality for management data, production processes, strategic plans, and the like. Therefore, business privacy may tend to increase economic output, at least in competitive industries. Signal theft has additional implications for the economic viability of many forms of telecommunications particularly in the entertainment area.

Factors affecting the supply of communications security include technical progress as well as legal changes. Both offer hope for more privacy in some areas, even as they threaten it in others. On the demand side, market failures can bring pressures for government to provide more privacy or security. Problems seem to arise most often when the information handler is a government or a firm with some degree of monopoly power. The claim that firms will use mistaken, stale, or irrelevant information is examined for both the competitive and monopoly cases. Fears along this line are probably less justified for the competitive case than for monopoly.

The paper reviews the economic rationale for government intervention and suggests that only when markets cannot work because of external effects, public goods problems, or economies of scale is there a compelling case for intervention. The need for police-like enforcement of laws in the telecommunications privacy/security area therefore is not always obvious.

A wide variety of remedies, only some of which require direct regulatory intervention, are available. The common law, privacy statutes, patent and copyright protection, administrative regulations, and self-protection are all possible solutions to information privacy and security problems, but they have different direct costs and different effects on economic incentives. There are good reasons to believe judicial enforcement of private rights of action often can be economically more efficient than administrative remedies as means of strengthening telecommunications security and privacy.

# Economics and Telecommunications Privacy: A Framework for Analysis

## I. Introduction

Privacy, and legislative proposals and academic writings about its protection, is today a veritable growth industry. The news media reflect almost constantly a concern that modern telecommunications, computerized data banks, and other products of the electronics revolution make intrusion so cheap and convenient that governments and businesses will be tempted to violate individual privacy on a scale never before contemplated. Less visible to the public eye has been a serious dialogue among government, business, and academic lawyers, engineers, and cyberneticists on the costs and other hidden drawbacks of various proposals for greater privacy. Yet systematic, published economic analyses of privacy issues have been rare. Moreover, we know of none devoted to telecommunications privacy issues. This paper is a first step in developing an economic analysis of privacy for telecommunications.

Our approach draws upon the "economics of information," which treats information basically as no different from the economy's other productive inputs like land, labor, and capital. Just as an economy needs labor, it needs information. And just as entrepreneurs invest in (physical) capital, they invest in information. Decisions to purchase

information yield to the same kind of economic analysis as decisions to purchase other factor inputs: A competitive, profit-maximizing firm will purchase information up unto the point where the expected payoff from the last bit of information equals its expected cost.1/ Some privacy statutes increase the costs of certain types of information or forbid their use altogether. 2/ Other statutes, like Section 605 of the Communications Act, tend in effect to decrease the costs of information or -- what is the same for economic analysis -- the costs of using certain information.

The domain of this paper is avowedly economics. Thus we focus mainly on costs and economic efficiency. We know other aspects and goals are important in the privacy arena. But we think these other factors do not diminish the relevance of an economic analysis of privacy, for at least two reasons. First, non-economic goals almost always have economic consequences -- usually net costs but sometimes net benefits. Second, many of the social norms governing us, including privacy norms, have arisen at least in part because they have always had economic

1/ A similar analysis can be applied to privacy viewed as a consumption good. An individual will purchase additional privacy as long as the additional (private) benefit exceeds the additional (private) costs.

2/ To forbid the use of a certain factor input is to increase its cost to infinity. Therefore the economics of information can treat the effects of the latter privacy statutes simply as special cases in a generalized cost-oriented framework.

consequences -- even though those consequences may sometimes not have been particularly obvious either to our ancestors or ourselves.3/

Let us state the case for the economic analysis of privacy in a slightly different way. To say that a specific privacy proposal increases the costs of certain information, even that it increases it to infinity, is not necessarily to condemn the proposal. Many important decisions in an area like privacy will, and perhaps should, remain "political" insofar as the public and their representatives wish to see them taken almost regardless of cost. Economic analysis should strive, we believe, to be neutral and aim chiefly to shed light upon the costs and benefits of specific policies. 4/ We think better knowledge of cost and benefits can lead to better policy decisions, whether or not the measurable costs exceed the measurable benefits.

3/ Economic analysis of "non-economic" institutions has been especially prominent in the work of Gary Becker and his colleagues. For samples, see Becker, A Theory of Marriage, 81 J. Pol. Econ. 813 (1973); idem, Crime and Punishment: An Economic Approach, 76 J. Pol. Econ. 169 (1968); or Amyra Grossbard, Economic Analysis of Polygyny, 17 Current Anthropology 701 (1976). The first formal applications of economic reasoning to the non-economic institution(s) called "privacy" are, so far as we know, in two important articles by Richard Posner, The Right of Privacy, 12 Georgia L. Rev. 393 (1978); and Privacy, Secrecy, and Reputation, 28 Buffalo L. Rev. 1 (1979). We draw heavily on Posner throughout Section II below.

4/ It is commonplace to observe (a) that neither economics nor any other social science can ever be 100 percent neutral about policy issues and (b) that economists (and therefore economics) often are flagrantly biased on all sorts of issues (not all of them "policies"!). We agree. Nonetheless, we think that by "striving," both economists and economics are frequently able to achieve neutrality for all practical intents and purposes.

In analyzing privacy issues, economics can usefully be taken well beyond the costs and benefits of specific information problems. We attempt below to extend it to the analysis of remedies. For example, whatever the immediate costs to the economy of restricting the gathering or transmission of certain information, total long-run costs may depend upon whether the restrictions are enforced primarily by judicial or administrative means; whether enforcement is primarily a matter of government or private action; and whether the remedies are based primarily on new laws or on extensions of old laws (like the patent and copyright laws or Section 605). Different approaches may use significantly different amounts of resources, both public and private, and they may set up different economic incentives. Hence we see a potentially fertile field for economic analysis.

Discussions of privacy, telecommunications security, and related policy issues run the danger of floundering among several different concepts. The most important concepts for the present discussion are three: (a) peace and quiet or, in the extreme, seclusion; (b) acquisition, storage, and dissemination of information about individuals or organizations, especially when the individuals or organizations have not authorized or do not know about such acquisition, storage, or dissemination; and (c) ability to exclude unwanted parties from access

to a telecommunications system.5/ Furthermore, the second concept may have quite different implications depending on whether one is dealing with individual or organizational privacy.

Economic analysis is relatively straightforward for the first and third concepts and, some might say, less interesting than for the second. Briefly put, peace, quiet, and seclusion can be not only important "inputs" to production, particularly for "intellectual" work, but also important "consumption" goods. And anti-theft provisions, which are at the heart of the third concept, seem absolutely essential for information-based and communications-based industries, in the same manner that our economy could hardly function without protection against physical theft. Therefore, it is the second concept of privacy that receives most attention below. (See Section II.)

Telecommunications privacy might seem at first glance to cover only a minor subset of the issues involved in privacy per se. The field of issues is much larger, however, to the extent that telecommunications includes matters like computer-to-computer links and penetration of data bases via electronic communications. Regulatory policy at the interface of telecommunications with computers is evolving rapidly, and it is not

5/ An important group of unwanted parties includes non-paying users of subscription entertainment media like pay TV. Although such theft-of-service issues are not viewed by most experts as privacy matters per se, they are generally thrown together with privacy under Section 605 of the Communications Act of 1934. Moreover, we think they are subject generally to the same sorts of legal and technical remedies as are privacy matters.

clear to us whether public policy in the coming decade is likely to, or should, draw a strong distinction between "computer privacy" and telecommunications privacy. Therefore, we do not separate them rigorously in this paper. Moreover, issues concerning the service records of regulated companies like common carriers and two-way cable systems potentially involve almost the entire range of personal privacy issues discussed below in Section II.6/

It is useful analytically to make a clear distinction between "privacy" and "security." The two terms are often used interchangeably, and this practice may lead to confusion. We take privacy to be a particular state of being or outcome (though not necessarily an end in itself). We take security to be a collection of devices and actions (including laws) that prevent unauthorized access to particular communications or information. Security devices and actions can at best provide remedies for only a subset of privacy violations -- those where unauthorized access is the main problem. But note that security may not provide

6/ The main communications technologies that may raise privacy concerns include (a) common carrier and other telephone and records transmission systems; (b) interactive video cable and similar two-way household systems for data retrieval and query; (c) cable, subscription, and pay TV and similar entertainment media (whether utilizing the radio spectrum or cables for distribution); (d) standard broadcasting; (e) data bases accessible by radio or cable communications; and (f) private radio services not included in the foregoing list. In the category of "cable" communications we include not only coaxial cables but also optic fibers, ordinary twisted-pair wires, and other transmission lines. Categories (a) and (b) are, we think, the most important for our discussion and subsume such services as electronic funds transfer, electronic mail, and computer-to-computer communications. Category (c) includes "theft-of-service" issues.

useful remedies where misuse of information by authorized persons is the main problem or where society may not wish to allow certain data to be gathered or maintained in the first place. In an important sense, then, privacy is a broader issue than security.

## II. The Economics of Privacy

According to Prosser's classic exposition, the invasion of privacy in law is not a unitary concept, but consists of four different torts united only by a common term. He distinguishes (1) appropriation of name or likeness, (2) intrusions, (3) public disclosure of (true) private facts, and (4) false light in the public eye.7/ We think a different breakdown is appropriate for analysis of telecommunications privacy issues. We shall discuss matters under the following four headings: (a) seclusion, or intrusions upon personal peace and quiet; (b) personal information, a heading that deals to some extent with all four of Prosser's categories, plus a set of activities he did not consider tortious, namely the gathering of or access to certain personal information without intrusion or where no clear misuse has yet occurred; (c) commercial and industrial "privacy"; and (d) theft of services via "intrusions" into telecommunications systems. Therefore we go beyond traditional legal privacy notions and consider the rights of

7/ William Prosser, Handbook of the Law of Torts, 4th ed. (1971), at 804.

corporations and others to protection from unauthorized appropriation of information transmitted by electronic signals.8/

A. Seclusion

The phrase "the right to be let alone" is the first formal expression of a right to privacy in English or American law.9/ It connotes one's being able to control his immediate environment (home or office) for uninterrupted reflection, repose, recreation, or relaxation. Of course, total seclusion is usually not desired or achievable; even Howard Hughes had to deal with a few intermediaries to achieve his goals. Yet there are at least two kinds of "economic" reasons why some right to seclusion is usually deemed appropriate.

First, "intellectual" workers and other "thinking" individuals require freedom from noise and interruption. Therefore some people may need private offices. Anyone who has worked in a high traffic, open area will confirm this point. It is important to note that this reason is an "instrumental" argument for privacy -- the protected individual becomes more productive as a result. From this point of view, privacy has no independent raison d'etre. The demand for privacy in this case is

8/ It seems the right of privacy, narrowly defined, pertains to individuals; a corporation traditionally has not been able to claim a right to privacy as such. See Prosser, ibid., at 815.

9/ Cooley, Torts, 2d ed. (1889), cited in Prosser, ibid., at 802.

derived from the demand for final goods and services. If we treat privacy (peace and quiet) as an intermediate good, it seems doubtful that substantial government intervention is required. It will be in the employer's interest to provide appropriate working conditions, based of course on the costs of doing so. To the extent workers independently desire additional privacy, it can be one of the fringe benefits in the overall wage package.

Second, privacy in the sense of seclusion -- perhaps as temporary withdrawal from the cares of society -- can also be desired for its own sake, that is as a consumer good. The increased demands for wilderness experiences in recent years presumably reflect desires for such solitude. But seclusion, for whatever end, is not a free good, and consequently we can never have all we would like. For example, wrong-number phone calls intrude on us. But to guarantee their elimination would require ridding ourselves of the phone or hiring an answering service -- both expensive alternatives. An unlisted number provides a certain degree of protection against unwanted phone calls, but only at the cost of reduced ease of access to the subscriber for other people. Even protection from unsolicited advertising or computerized dialing techniques involves a cost since sellers would have to turn to less efficient methods of reaching potential customers.

Privacy as a consumption good is protected to some extent by postal regulations, and similar protection from "junk" phone calls has been

sought.10/ In summary, however, we doubt that privacy-as-seclusion will occupy a major place on the agenda of telecommunications privacy issues, compared to the three areas we discuss next.

B. Personal Information

No issue in the privacy sphere generates more emotion and concern than the possibility that information about the lives and habits of individuals will fall into the wrong hands or otherwise be subject to misuse. In an interconnected computerized age, there is little doubt that there exist new technical capabilities for extensive information gathering, collation, and distribution. Indeed in some cases, individuals may not even be aware information about them is being collected. To put the matter in the starkest possible terms: "The fundamental problem ... is that the information age will rob each one of us of one of our more important rights in a free society: The right to privacy."11/ In the sphere of telecommunications policy, personal information issues seem likely to arise particularly in connection with service records of regulated companies, for example, in telephone and

10/ Postal patrons may ask to have their names deleted from mailing lists of offensive material. Automated dialing techniques and other unsolicited calls have moved some people to suggest regulation of such "junk" calls is needed. See FCC Docket 78-100, Report and Order, May 22, 1980. The FCC has declined so far to take any major action, largely because there is no evidence unsolicited interstate calls (the only calls under FCC jurisdiction) are as yet a real problem.

11/ Chairman Charles Ferris, Federal Communications Commission, speech before the Union League Club, New York, October 13, 1980.

cable television. We think the aspects of personal privacy we discuss next may well be relevant in analyzing the appropriateness of new privacy regulations in an emerging technology like interactive (two-way) cable.

1. The Economic Value of Personal Information

Information is essential for most personal and business dealings. Life is pervaded by contacts and various relationships with other people, and we could not (indeed most of us would not) have it otherwise. We deal with friends, employers, lenders, government offices, merchants, and a host of others. In all these cases, we engage in transactions -- the obligations of friendship, personal services, money, and the like. In order for these transactions to be efficiency-increasing, it is important that the terms of agreement and exchange be understood by all parties involved. And the parties must have (at least implicit) understandings about enforcement.12/ But since it is neither possible nor desirable to have complete and fully enforceable understandings, the participants normally acquire at least some information about one another. The amount of information will depend on the complexity of a relationship, its expected duration, and the degree to which each party has to rely on the other.13/

12/ This does not necessarily mean compelling the completion of the terms of a contract; it simply requires that full damages be paid in case of breach.

13/ "Amount" may have both a quantitative and a qualitative aspect.

For example, a restaurant normally gathers no information about a patron other than what can be obtained by a casual glance. If the customer wishes to complicate the transaction by charging the meal, he will be required to identify himself, and information about his current credit status will be gathered. At the other extreme, an individual seeking a high-level, sensitive position must reasonably expect that he will have to provide a great deal of information about himself and that it will be subject to cross-checking and verification. Indeed, in the latter case, what constitutes relevant information may not be definable or specifically targetable in advance of the actual data gathering. A "background" check constitutes, from some points of view, just such a "fishing expedition." It is intuitively clear that there will be at least some cases where very extensive information gathering is justified. Can we identify the kinds of information likely to be of interest and the conditions under which the correct amount of information will be forthcoming before of the data collection itself? Even raising the question suggests that for some purposes, it is hard to imagine any reserved area of privacy, save in the confines of one's own mind. To take the extreme case, if the CIA is recruiting a double agent it will attempt the most probing information gathering conceivable. The interest will surely extend to political views, sexual proclivities, and

similar matters. The essential economic point is that resources may be used inefficiently in the absence of sufficient information to evaluate them properly.14/

For example, suppose a law (or court decision or administrative ruling) moves a certain category of information into an "unrequestable" category. The former user can (1) disobey the rule, thereby incurring costs if the rule is enforced 15/, or (2) he can avoid it by turning to substitute (legal) sources of information. These new sources will necessarily be of poorer quality.16/ In either case, the net effect is likely to be lower productivity and (total) income.

Consider another example: Suppose an employer simply assigns job applicants to positions in the order that vacancies occur and as people apply for positions. That is, he does it in an essentially random fashion, making no use of information about the applicants. The

14/ George Stigler, An Introduction to Privacy in Economics and Politics, University of Chicago Center for the Study of the Economy and the State, Working Paper No. 010-1 (1979), at 13.

15/ The expected costs for a risk-neutral individual will be the penalty for violation multiplied by the probability of being convicted.

16/ If the new sources were of equal or better quality, they would have already been used by a profit-maximizing firm. Since the new sources are not perfect substitutes for the old ones, costs rise, less information is gathered, and the quality of decision making declines. Thus the availability of alternative information sources does not alter the earlier point concerning efficiency loss. The objection that the information formerly collected was irrelevant to proper decision making is dealt with later in the paper. See Section VI.

consequence is that most, perhaps all, individuals will be poorly suited to their jobs. Productivity will be low, and as a consequence employment, wages, and incomes will all be lower than would be the case if information about worker characteristics were allowed to influence the job assignment. Analogous arguments can be made for credit, insurance, and other services. Therefore, before one criticizes any particular information-gathering practice or recommends legal restrictions upon it, we believe he should analyze carefully the economic functions that practice may serve.

2. The Distributional Impact of Information Restrictions

There will also be effects on income distribution from the prohibition on information gathering. Consider the employment case. If firms are not allowed to collect detailed information about specific characteristics of individual employees, they will still learn the average productivity of the people they hire and will of necessity base wage decisions on this inferior knowledge.17/ The result will be a "leveling" effect, whereby highly qualified people will receive lower wages and less desirable positions than they could otherwise command, and modestly endowed individuals will receive benefits beyond those an unimpeded market would provide. So there will occur a transfer of

17/ We are again, as elsewhere in this paper, abstracting from the problem of risk.

wealth from more highly qualified individuals (as well as customers and owners of firms) to the less qualified.

This distributional aspect of privacy says simply that there are strong economic incentives for some individuals to control personal information, in order to cast themselves in the best possible light. Indeed, Posner has argued that much of the so-called desire for privacy is in fact a manifestation of this proclivity.18/ However one feels about the overall importance of this determinant of the demand for privacy, it will clearly be important in at least some circumstances. Thus, proposals for systematic increases in records privacy should be scrutinized to analyze the effects on income distribution as well as on the economic efficiency of labor and product markets.

3. Privacy as a "Consumption" Good

While the previous (implicit) argument against legal restraints on information collection seems to us fairly compelling, it is not

18/ Richard Posner, The Economics of Privacy, Regulation, May/June 1978, at 22.

conclusive.19/ Privacy for its own sake may legitimately be desired by society.20/ If so, the inefficiencies generated in labor markets, credit markets, and elsewhere may simply be regarded as a price we must pay for a desired service. But we should always remember that there are no free lunches: more privacy means less of something else. And in the absence of any independent method of valuing privacy as a consumer good, there may be no good way of knowing precisely whether the cost is commensurate with the benefits derived.21/ In analyzing privacy proposals for telecommunications, or any other industry, the body politic should not neglect these complications.

19/ We are not discussing the methods by which a given class of information is collected. Clearly, some of the possible means of collection are seen by society as impermissible. And among commentators like Posner, who express a great deal of skepticism about many current proposals on privacy, we know of none that question basic prohibition against wiretapping, trespass, and similar intrusions.

20/ For the moment we abstract from the potentially serious problem of narrow interest groups seeking "privacy" protection for themselves in contradiction to the overall societal interest. If there are public goods aspects to the provision of privacy, the problem is magnified even further.

21/ On the other hand, for modestly qualified individuals to receive benefits beyond those a well-informed market would bestow, as well as the reverse, cannot be defended on any fairness criteria we know. And there are other dimensions to the efficiency effects. Extensive information gathering may inhibit the production of illegal goods and services. On the other hand, it may have a "chilling" effect on the consumption of legal, but morally ambiguous, goods and services (e.g., abortions, pornography).

## 4. Voluntary Versus Involuntary Provision of Information

Another major personal privacy issue is the extent to which the provision of information about an individual is voluntary. There are three possibilities. First, information may be obtained in a clearly coercive way. Most pure examples are in government settings; for example, we are all required to disclose financial information to the IRS and a wide variety of personal information to the Bureau of the Census. The requirements are absolute, conditional only on our citizenship or presence in the United States. There are penalties for noncompliance, and no right of information privacy is recognized by society in this context. (That is, we are not allowed to keep certain information from IRS or Census. But they, in turn, are subject to heavy restrictions against release of personal information.)

A second, but less extreme, case occurs when we deal with a monopolist. If the service we are purchasing has only a few or very poor substitutes, we may have no choice but to provide highly personal information to the supplier. An example might be a credit bureau (if credit is as essential as some feel) or the telephone company. The "compulsion" stems from the fact that doing without the service in question would be very costly (the substitutes are very poor).

Whenever there is monopoly, there is a greater probability than under competition that too much information will be gathered. The reason is

that the element of compulsion allows the collector of information to shift some fraction of the costs onto the provider. Since the demander is not paying the full price of the information, he will tend to demand a larger quantity than is justified in view of the real social costs of providing it. The government seems likely to be the worst offender: the SEC collects reams of (mostly irrelevant) data about companies, the ICC about the details of railroad management, the Federal Reserve on the details of certain financial transactions, and the list is endless. In none of these cases are the costs of data collection and transmission in the agency's budget; hence, there is little incentive to take account of the true cost.22/ The failure will be less serious, but still present to some degree, in the case of the private monopolist. His requirements for information raise the price of doing business with him and reduce his sales; this reaction puts a partial limit on monopolist's demands. Monopoly can be thought of as a kind of market failure in this case. It is well to note, however, that failures of this type usually originate in government itself or in the requirements it imposes on others.

The third situation occurs when information about individual A is transmitted to B, who in turn passes it on to C. The second transmittal, if it takes place without permission or in contravention of

22/ There are at least two reasons why. First, the agency is typically not a profit maximizer, so even if the cost were in the agency's budget there would still be no incentive to optimize on the same basis as firms. Second, higher costs might simply be used to expand an agency's size and range of tasks performed internally.

an implied agreement of confidentiality, may involve a type of compulsion. The feature that distinguishes this situation from the previous one is that the information in question has already been placed in the hands of a second party. If there is a problem, it is probably better viewed as one involving an incompletely specified agreement between A and B or as an enforcement problem in contracts.23/ Whether A had a right to rely on B's discretion is of course an issue that could be litigated.24/

In competitive situations, that is, where all parties have a reasonable range of alternatives, there is a much stronger presumption that the amounts of information provided and received will be the "right" amounts. Providers of information will be able to purchase the desired degree of privacy (perhaps by accepting lower incomes or lower product quality) and demanders will also get the information they want (possibly by paying higher wages or prices). Those with strong preferences for privacy will work for firms where little personal information about employees is needed. Those with fewer concerns about divulging facts on themselves will face a richer array of job opportunities.

23/ Perhaps because it is too costly to contract more completely or to enforce contracts of the type.

24/ A large group of interesting uses falls under this heading. If a pollster discloses your answer to a question to a third party (with an identification tag), there may be a violation of a privacy expectation. Similarly, if a credit card company discloses your purchase patterns to the other merchants, a problem may arise. A primary problem in these instances, of course, is that it may be difficult to know whether the information has been revealed.

When the price mechanism is functioning efficiently, employers that place excessive demands for information on employees will have to pay higher wages, and therefore they will have incentive to collect only information truly useful to them. Similar arguments hold for insurance, credit, banking, or any other market, including markets for various telecommunications services. That is, competitive pressures normally will encourage businesses to collect only information with real economic value. So government-mandated restrictions on information will tend, in workably competitive markets, to reduce national income. Whether there is a case for government intervention depends on (1) the extent of market failure and (2) the likely costs and benefits of government action. We think intervention should be justified only on a case-by-case basis, always with the awareness that one man's privacy may be another man's lost wages.

C. Commercial and Industrial Privacy

Commercial and industrial privacy raises somewhat different problems from personal privacy. In no sense is commercial privacy a consumption good. Its importance is entirely instrumental. That is, it is most properly regarded as an input to production.25/

25/ We recognize that it may be difficult to distinguish the demand for commercial privacy from the demands of owners and managers for personal privacy. For a general discussion of the problem of owners' and managers' goals in a firm setting, see Armen Alchian and Reuben Kessel, Competition, Monopoly, and the Pursuit of Money, in Aspects of Labor Economics, National Bureau of Economic Research, Special Conference Series, Vol. 14, Princeton University Press (1962).

Certain classes of information are explicitly recognized as proprietary and are protected by the patent, trademark, and copyright laws. Patents have a seventeen-year period of protection, to encourage above normal returns to new processes and hence stimulate innovation. If competitors are free to copy a new method without delay, the incentive to invent may be diminished.26/ The copyright laws offer similar protection to authors and composers. Again, the protection is justified in terms of the overall benefits to society. Analogously, trademarks play useful social roles by carrying signals on the quality of goods and assigning responsibility for defects.

Business firms may also have secrets not protected by patents or copyrights. For a variety of reasons, such protection may not be legally available for certain classes of information, or the firm may prefer nondisclosure of some process or product. To the extent these secrets are valuable to the firm and to society, there is a societal as well as private interest in their security. Strategic plans, new product developments, bids, prices, planned responses to competition, and many other things fall under this rubric. Common law and statutory law recognize a right of privacy in trade secrets and offer remedies if the security of a firm is breached by certain methods. For example, industrial espionage is punishable by law, and properly so.

26/ This is basically an empirical question, on which the evidence is equivocal.

A further government role may be hard to defend, unless there is convincing evidence of a specific market failure. A firm can be expected to take protective action up to the point where the additional cost of doing so is equal to the additional benefit. Spillovers of either costs or benefits seem unlikely. So if one sees a firm transmitting proprietary information over an unencrypted channel, for example, he is probably justified in believing the benefits of protection simply are not worth the cost.

D. Theft of Service

A fourth problem is intrusion upon a communications system to intercept and use subscription entertainment signals. While one may tend not to think of this matter as a privacy issue, it shares a number of features and potential methods of solution with other telecommunications intrusions, particularly those related to commercial privacy.27/

Some firms provide signals intended only for paying recipients. Normally these signals are encoded or difficult to receive in some way,

27/ In fact, the authors believe that for most analytical purposes there is little reason to distinguish between theft of entertainment services and theft of commercial and proprietary information in electronic form. We make the distinction here merely because it has to date been conventional in most discussions of telecommunications security, even though both entertainment signals and point-to-point information channels are protected primarily (and without distinction from one another) by Section 605 of the Communications Act.

and paying customers are provided with a decoder or special receiver. Anyone who can obtain such equipment from another source can also receive and use the signal -- without paying. Such opportunities present obvious problems for the providers, but thus far it has proven difficult to enforce property rights in broadcast signals before the courts.

The troubles of MDS (multipoint distribution service, which operates at microwave frequencies) and subscription TV (STV) provide examples. Entrepreneurs such as "Pirate Electronics" (a recently formed Arizona corporation) market decoders so that receiver owners can watch the subscription programs without paying. At the moment the legal status of this practice is unclear.28/ Courts in Detroit and Phoenix have granted preliminary injunctions barring the sale of unauthorized MDS instruments; but in a Los Angeles STV suit, it was held there was no cause of action in airwave piracy.29/ As a consequence it is not known definitively what legal rights of action exist to protect entertainment signals. The issue also presents a problem for cable and potentially

28/ The "practice" has two aspects: (1) the viewer taking the signal off the air and decoding it with his own "black box" and (2) selling the decoders themselves. If the first practice is legal, then presumably the second is also. It is not clear that if (1) were illegal then (2) would be also. For obvious enforcement cost reasons, the STV industry has chosen to bring its actions mainly at the manufacturing level.

29/ Business Week, September 29, 1980, at 44. The distinction seems to hinge on the fact that the FCC treats STV as a form of "broadcasting" and MDS as a common carrier service. Broadcasting is not covered by Section 605, but common carrier services are covered.

for satellite broadcasting.30/ Until this issue is decided (probably by legislation), perhaps the phrase "unauthorized use of service" is better than "theft of service." The real issue(s), we think, should not be "theft," but (a) the circumstances where subscription media are desirable components of a communications package, (b) whether it is necessary or desirable that non-payers be excluded, and (c) who should be responsible for policing. On the last point, it is by no means clear that governmental authorities are necessarily in a better position to provide signal security than the programmers themselves via encryption or other self-protective means. (See Sections V and VIII below.)

## III. The Demand for Information Security

Individuals and society normally should want to pay for security or to seek new laws guarding privacy only when there are real threats of intrusion or information misuse. That is, one can imagine almost an infinite number of abuses; yet it is impossible to protect against all of them. Therefore individuals and society face substantial allocation questions in deciding where to invest their limited resources in physical security, legal protections, or simple (but not costless) caution. The greatest threats, measured in terms of their total monetary and non-monetary costs, presumably deserve the greatest

30/ A number of states have already enacted antipirating statutes for cable.

protective investments.31/ Even though many important costs of protection or threats may not be measurable, we think this framework is useful for analysis. Furthermore, we suggest society can generally be looked upon as constantly making such cost comparisons, if only implicitly. That is, enactment of any new law restricting data access implies a legislative judgment that the estimated costs imposed by the restiction are less than the ultimate total costs of the abuses it would stop.

For the purpose of demand analysis, we reclassify potential invasions of privacy into two large categories: (a) where the intruder is a government, or an organization or individual seeking information for essentially political purposes; and (b) where the intruder is an organization or individual acting without political motives. Non-political intrusions may be motivated by commercial ends, by "idle curiosity," or by extortion and blackmail. Commercial intrusions may be subdivided according to whether they are done by (1) monopoly firms or (2) competitive firms.

31/ We stress our broad view of costs, both for protective measures and for threats. For example, a particular law or regulation may require no direct investment costs, yet the costs it imposes may be substantial over the long run in terms of lost production. Such situations involve what the economist calls "opportunity costs." And the ultimate costs of threats to security may be direct monetary costs, opportunity costs, or (non-measurable) psychological costs.

Although there are many exceptions in specific cases, we think as a general matter that abuses by individuals and competitive firms will be most amenable to judicial remedies and self-protection. On the other hand, we think abuses by governments, by others acting with political motives, and by monopoly firms are most likely to require administrative remedies ("regulation"), prior restraints, and public expenditures. Our reasoning basically is that governments (which essentially are monopolists -- their most important monopoly being the right to use coercive violence) and monopoly firms have weaker incentives to protect information properly than do competitive firms. Furthermore, we suspect individuals acting without organizational support (including the computers and telecommunications equipment that normally are too expensive for individuals) simply do not constitute a massive threat to privacy.32/ Competitive firms that do not protect information about their customers or that do not provide secure communications channels will, if there is widespread public demand for privacy, have difficulties surviving in the marketplace. Customers who want certain kinds of privacy, like unlisted numbers or assurances that buying habits data or mailing lists will not be sold, should be able to shop around for companies with reputations for discretion. But when a monopoly firm or a government does not provide the level of protection the individual wants, then the individual may have nowhere to turn. Hence our

32/ Although opinion polls show a high level of public concern over privacy issues, we are aware of no systematic research that satisfactorily documents the problem.

conclusion that regulation and prior restraint to guard privacy may be needed more in monopoly and governmental contexts than when one deals with possible privacy violations by competitive firms or by individuals.33/

Absent political involvement or monopoly, demands for government intervention to safeguard privacy may also arise from additional market failures. Therefore let us examine the potential seriousness of several alleged market failures that often serve as arguments for government mandated privacy protection. They include the following: (1) mistaken or outdated information; (2) stale or superseded information; and (3) irrelevant or improper information.34/

Recall first that the economic purpose of information gathering in most cases is to enable correct, i.e., value-maximizing, decisions. Second,

33/ There are two categories of abuse that we think cut across the four categories of potential abusers, such that remedies probably should not differ according to whether the abuser is a government, a monopoly firm, a competitive firm, or an individual. These two categories are (a) misuses of (true) information that are illegal under the common and statutory law of extortion and (b) those intrusions that are essentially forms of trespass. The laws covering extortion and trespass may well need to be strengthened in the face of ever-developing computer and telecommunications technologies. If so, however, we believe these remedies should be seen not as part of a new body of privacy law, but rather as additions to important existing branches of the tort law.

34/ Stigler, op. cit., at 5. We call them "alleged market failures" not only because they are unproven, but also because they do not fit easily into the economist's traditional categorization of market failures as (a) economies of scale and (b) externalities. See Section V below, esp. notes 41-47 and accompanying text.

keep in mind what is meant by market failure. In the case of mistaken or outdated information, there is failure if an information-gathering entity fails to correct an error when either the subject or the information purchaser would be willing to pay a price in excess of the cost of correction. While this kind of market failure is imaginable, there are strong incentives for firms to keep the problem within bounds.35/ Inaccurate or outdated information leads to mistakes, and mistakes hurt profitability or the achievement of other goals. No firm wishes to accept bad customers (or employees) and turn away good ones. The information firm that supplies bad information will itself soon find that it is losing customers.36/ While perhaps almost everyone has heard horrendous examples of this type of error, we have seen no systematic evidence to support the notion that it is widespread.

The second type of error, the use of stale information, represents a somewhat different type of market failure. The standard example is the use of an old (10 years, 20 years?) arrest record to deny an applicant a job or credit. The implicit inference is that the potential employer or lender is unable to filter out the information most useful for his

35/ Of course, the error rate will never be zero. The reason is that the costs of insuring a zero error rate would exceed the benefits.

36/ If the information firms' customers cannot detect the bad information sufficiently quickly, a problem may remain. They may learn of false "goods" more rapidly than false "bads". Failing to hire good employees shows up only indirectly, and in the long run, in the form of a reduced ability to compete, whereas bad employees will be detectable reasonably quickly.

decision.37/ Perhaps firms do fail to maximize profits in situations like this, or are simply irrational, but the incentive to earn high profits is a powerful force against using improper information. An alternative hypothesis is that the information alleged by some to be irrelevant is useful at least to some degree. George Stigler notes that, as usual in this kind of argument, there is no evidence presented for either side.38/

The use of irrelevant or improper information may be simply a variant of the second problem if the firm is a profit maximizer. If, however, the firm discriminates on the basis of sex, race, or some similar characteristic, things become much more complicated. In particular, if race, sex, or similar characteristics are irrelevant to productivity, there is then a pure discrimination problem that society may wish to deal with as such, rather than as a privacy matter. We suspect some of the more extreme privacy concerns about "irrelevant" information may be overdrawn; but since there is so little knowledge on the subject, we remain open to new evidence.

37/ If information is gathered centrally (as by credit bureaus) and provided in its entirety, a report may contain information not of use to a particular subscriber. It may be cheaper for the information firm to send out a standard package rather than tailor the product to each request. A profit maximizing user will simply filter out (ignore) information irrelevant to its purposes.

38/ Op. cit., at 7.

To sum up our view of the demand for privacy, we think the felt needs for privacy safeguards are likely to be strongest in governmental and monopolistic settings and weakest in competitive markets. And specifically we are skeptical that such alleged "market failures" as mistaken, stale, or irrelevant information are likely to be pervasive where competition is healthy. Therefore we would not be surprised if society should allocate most of its "privacy protection resources" to the government and monopoly sectors.

## IV. The Supply of Information Security

Information security is produced from a variety of inputs, employed in ways determined by costs and available technology. At any time there will be a number of techniques available, including coding, encryption, physical protection, audit trails that reveal who has had access to sensitive information, procedural rules for employees, and legal remedies. These techniques may be as simple as remembering to lock the door, but others are "technical" in the ordinary sense of that term. Thus, a change in knowledge (say, in mathematics) may make feasible and widely available protection that could not have been contemplated ten years ago. Specific new technologies will always have the effect of lowering the costs of protection. They may seem inexpensive in some absolute sense, but they will never be adopted unless they are cheaper than other technologies. If an older method is truly a cheaper way of providing a given amount of security, it will not be superseded by the

new method.39/ New specific technologies include public-key cryptography, very large-scale integrated circuitry, and fiber optics.

Rules on legal actions open to information protectors play roles analogous to technology. Laws forbidding (say) wiretapping increase the of security of telephone conversations.40/ Patents, copyrights, the common law of trade secrets, Section 605 of the Federal Communications Act, other statutes, and a number of the rules of the FCC may serve in similar ways. The effects of such rules will not be simple, however. To some extent, rules are substitutes for self-protection. This fact leads to several possibilities. The first is that if a law protecting information is enforced by public authorities, firms will be able to relax their own efforts at self-protection. The resources they had been employing for this purpose will now have a higher value in some other use. In this instance private and publicly provided security are substitutes. A second possibility is that the two forms of protection complement each other. In this case the passage of a law enhances the productivity of the protective activities of the firm, and more private steps will be undertaken. One example might be as follows: If the law affords you a remedy, say in the form of an action for damages, you may

39/ Technological change can cut both ways, however. Developments in code-breaking and decryption, other things held constant, will raise the cost of security, so that less security will be produced at a given cost.

40/ Obviously no claim is made that this or similar laws provide perfectly secure communications, merely that they move in that direction as a first approximation.

be more likely to mount a search for an intruder on your privacy than if it does not. In any event, there is always an incentive for a firm to seek government assistance in providing protection. Where the costs of a court action are low and can easily be assigned to the parties involved, there may be a good case for the government to create a private right of action. In other instances the desirability of governmentally provided protection will depend on the costs of providing and enforcing rules and on how the burden of those costs will be distributed if the government is the protector.

## V. Economic Reasons for Government to Supply or Regulate Goods and Services

The commodity or service we have labeled communications "security" can be provided by governments, by private entrepreneurs and business firms, or by some combination of the public and private sectors. There is a well established body of theory, primarily developed in that branch of economics called "public finance," that offers guidelines on the roles of governments as (a) suppliers of goods and services or as (b) regulators of their production and sale.41/ The situations where intervention (via either regulation or outright government ownership) is

41/ That is, guidelines for governments that wish to be economically efficient. In this paper, we have chosen not to analyze situations where governments are mainly pursuing goals other than economic efficiency. However, we suspect that the explicit pursuit of such goals would not substantially alter our conclusions or the mode of analysis we present in this paper.

usually deemed appropriate all come under the broad heading of "market failure." The two main categories of market failure are economies of scale and externalities.42/

Economists generally assume most goods and services are produced under conditions of increasing costs ("diseconomies of scale") or constant costs ("constant returns to scale"). Industries that produce such goods or services are candidates for competitive organization.43/ But on the other hand, industries that produce goods or services under conditions of decreasing unit costs ("economies of scale") are candidates for monopolistic organization. These industries are the so-called "natural monopolies" -- often thought to be public utilities like electricity, telephone service, and railroads. We hasten to add that this conventional wisdom has undergone a good deal of questioning in recent years.44/ But if indeed such industries are characterized by scale economies, it is at least conceptually possible that with proper

42/ Some recent literature identifies "economies of scope" as another category that justifies government intervention. To the extent this categorization is valid, we think its policy implications in our present context are not significantly different from the implications of scale economies. Therefore we do not treat economies of scope as a third category of market failure. See W. J. Baumol, On the 'Proper' Cost Tests for Natural Monopoly in a Multi-Product Industry, 67 American Economic Review 809 (1977).

43/ We shall not give an explanation here. The routine arguments may be found in any standard economics principles textbook. See, for example, Paul Samuelson, Economics, 9th ed., McGraw-Hill (1973), at 147-161.

44/ See note 56 below; also cf. Nina Cornell and Douglas Webbink, Common Carrier Regulation and Technological Change: The New Competition in the Communications Industries, U.S. Congress, Joint Economic Committee, forthcoming (1981).

controls, society might benefit from their being organized as monopolies. The reason is that unit production costs will be lower under monopoly than under competition. But an uncontrolled monopolist presumably would charge a price far above his actual production costs. Hence the common argument for government licensing and control, or ownership, of natural monopolies.45/

"Externalities" exist when the producer of a good or service does not bear the full social costs of his productive activities or when he does not reap fully their profits. Pollution is the most common example of the former. Invention and other innovative activities are common examples of the latter. For instance, the economic incentives for research and development may be weak in areas where the difficulty of enforcing patent protection does not allow inventors to capture large rewards for their work. This possibility leads to the argument for government management of activities like agricultural research, where effective patent protection is often virtually impossible yet where social benefits may be potentially enormous.46/

---

45/ The arguments for government ownership vs. regulation may hinge upon political considerations, incentives for economic efficiency, or a combination.

46/ And, of course, the patent system is itself an important type of regulation -- albeit not "public utility" regulation -- and an important alternative to direct government ownership of research and development facilities.

"Free rider" situations are a special class of externalities, and they often involve "public goods." Public goods have the characteristic that one person's consumption does not diminish potential consumption by others. For example, compare a loaf of bread to the Washington Monument. If I eat the bread, you cannot. But if I look at the monument, I diminish neither the services it provides nor your ability to consume them. Hence monuments are public goods and loaves of bread are not. The inability of firms to restrict access to and hence charge for public goods means they normally will not supply such goods -- at least not in amounts commensurate with the benefits they confer. So public goods often are owned or produced by the "public" through its government. For example, fire prevention is usually treated in cities as a public good, due to a free-rider problem. In a crowded city without a fire department, most homeowners might buy fire protection from private entrepreneurs. But the non-purchasing homeowners will also receive substantial safeguards if most of their neighbors buy protection, simply because the major fire hazard in a crowded city is probably the spread of conflagration from building to building. Such free riding strikes most of us as blatantly unfair; moreover it may be economically inefficient. And it provides a rationale for governments to operate fire departments.47/

47/ An obvious alternative would be to require every homeowner to contract with a suitable firm for fire protection. This line of analysis does not hold, however, for suburbs and rural areas where there is little danger of fire spreading from building to building.

Information is a public good and therefore subject to important externalities. Specifically, the producer of information often is unable to capture the full profits his information might generate. Moreover profitability, in a competitive market, is an important measure of the value society places on an activity. Therefore, the inability of information producers to profit adequately from their activities may lead to underinvestment in certain information producing activities, as measured from society's point of view. The patent and copyright laws aim, in part, to alleviate this problem. Furthermore many types of information -- much scientific research, technical data, economic statistics, agricultural market information, consumer information -- are produced and distributed primarily by government agencies precisely because of their public goods characteristics.

## VI. When Should Law Enforcement and Other Protection of Rights Be Government Functions?

One may have a reflex that says, "Law enforcement is always a government function. Society's decision to follow this approach is political and even moral or philosophical. Therefore, economic analysis has no role here." We would not even be surprised if a majority of economists subscribe to such a view. But there are economic arguments for

government management of much law enforcement.48/ They are grounded in the traditional economics of public finance (outlined above in Section V). The two most important arguments relate to economies of scale (especially in investigation) and free riders (especially where deterrence is concerned). Significant scale economies or substantial free rider problems in law enforcement may then constitute sufficient (but not necessary) conditions for public management. 49/ Conversely, we think the case for government provision of law enforcement services is weakened where important scale economics or externalities are not demonstrable.

For an example of scale economies, consider the area of criminal investigation. Because the professional criminal tends to repeat a successful crime and thereby establish a modus operandi, there is a high probability that investigators will detect a pattern leading to apprehension. But victims of the repeat criminal are likely to be

48/ It should be recognized that the virtual government monopoly in enforcement of criminal law is a relatively recent phenomenon in Anglo-American jurisprudence. For example, private bounty hunting was common until the late nineteenth century as a means for apprehending criminals. And English law still allows private enforcement against certain classes of crime, like shoplifting. Almost all private enforcement of criminal law has been legislated away in the United States. For a fascinating survey, see William Landes and Richard Posner, The Private Enforcement of Law, 4 J. Legal Stud. 1 (1975).

49/ Landes and Posner, op. cit., argue that public enforcement may be preferred to private enforcement even in the absence of scale economies and free rider problems, due to the phenomenon of "overenforcement" in certain contexts. It is important to note, however, that their objection to private enforcement in such cases is economic rather than political or moral. See note 53, below.

scattered, out of touch with one another, and maybe even dead. Each knows only a small piece of the puzzle. Furthermore, the economic payoff to a single victim who investigates a crime successfully and obtains a conviction would normally be very small in relation to the costs of investigation, apprehension, and prosecution. Only investigators whose activities span a large number of criminal incidents are likely to have enough information to "put it all together" at a cost society would find acceptable.50/ Hence the possibility of substantial scale economies in investigation is one important argument for government control of the "natural monopoly" called "law enforcement."51/

Potential free rider problems for law enforcement arise perhaps most significantly in the deterrence of crime. Consider a mythical village of fifty homes and no public police force. If, say, forty-five homeowners should contract with private security companies to patrol their properties, then we think the remaining five homeowners would probably get "free rides" and could feel relatively safe against thieves and other assorted criminals--especially to the extent that the free

50/ Although private enforcement of criminal laws is generally forbidden expressly by statute in the United States, many crimes are simultaneously torts. E.g., the crime of theft is also the tort of conversion. But in addition to the costs of investigating and prosecuting such torts, the victim is likely to find the thief has few readily attachable assets! See Landes and Posner, op. cit.

51/ The reader may wish to ponder why police departments in the United States developed as branches of government rather than, like telephone companies, regulated public utilities. But see note 53 below.

riders can conceal their identities from potential criminals.52/ We submit that such free ride potentials are a major justification for today's accepted approach to criminal law enforcement, i.e., virtual government monopoly.53/ And in parallel to our discussion of scale economies immediately above, we think the case for government provision of law enforcement services is also weakened where a substantial free rider problem is not demonstrable.

Undoubtedly there are cases involving telecommunications or information privacy where scale economies and free rider arguments justify some measure of government enforcement of criminal laws, as in the example of the mythical village just discussed. But we believe these issues should be approached on a case-by-case and technology-by-technology basis. We are particularly unwilling a priori, and without strong logic or evidence, to accept the notion that government enforcement should be the general case in matters involving telecommunications privacy. In summary, we are skeptical that police-like law enforcement in the

52/ Note that all the homeowners, not just the five free riders, have an incentive to conceal the free riders' identities in order simply to reduce the village's overall attractiveness to outside thieves.

53/ A third reason for government monopoly in law enforcement, beyond the rationales of scale economies and free riders, has been advanced by Landes and Posner, op. cit. Their argument is that private, competitive law enforcement "firms" -- like the bounty hunters of yore -- will invest too many of society's resources in law enforcement and therefore will be economically wasteful. Although we have no major quarrel with the Landes/Posner analysis on its own terms, given their tightly confining assumptions, we are not convinced their "bounty-hunter" model applies in any important way to telecommunications. So we do not concern ourselves here with their arguments.

general area of telecommunications and information privacy is likely to offer many significant advantages over a well thought out system of self-protection and private enforcement. This hypothesis is bolstered by our belief that digital electronics technologies may soon reduce encryption and self-protection costs significantly.54/

## VII. The Economics of Remedies

The need to conserve law enforcement resources is general -- not limited to telecommunications issues or to privacy. Moreover, this need encompasses private resources spent for security and enforcement of rights, as well as public expenditures. The latter point seems to us especially important. A policy that simply shifts the costs of protection from the public to the private sector is not necessarily good if, for example, it should also cause a large increase in the total (public plus private) costs of information security.

54/ Our skepticism about economies of scale in enforcing communications security laws parallels a relatively new skepticism among regulatory economists about natural monopolies and economies of scale in many important areas. For years, and until recently, the notion of scale economies was often accepted uncritically, without evidence, as the main reason for government intervention in a host of industries. But, we believe, such routine belief in natural monopoly is fading. Cf. FCC Docket 20003, Second Report, January 9, 1980, esp. paras. 108-118. Also, Nina Cornell, Daniel Kelley, and Peter Greenhalgh, Social Objectives and Competition in Common Carrier Communications: Incompatible or Inseparable? Working Paper No. 1, Office of Plans and Policy, Federal Communications Commission (1980).

It is tautologically true that where there are no economies of scale or externalities in providing security, the total costs of a decentralized private security system will be no greater than a totally public system or a mixed system.55/ Furthermore, as a practical matter, we think a private system will tend to have lower total costs for at least two other reasons: (1) public systems are likely to suffer from problems of bureaucratic inertia and coordination, given their lack of profit-and-loss incentives; and (2) private systems allow people and firms to pick only the amounts of security they feel they need, rather than impose a uniform (highest common denominator?) cost on everyone.

Judicial enforcement of privacy rights seems to us preferable to administrative enforcement (i.e., continuous regulation) in industries and markets not characterized by scale economies or externalities in either the industry's production per se or in provision of information/telecommunications security.56/ This distinction corresponds generally to that customarily made between industries where antitrust is the primary means of economic regulation and those where regulation is (in the United States) primarily by independent

55/ We are prepared, as noted above on p. 39, to grant the possible existence of market failure in provision of telecommunications and information security on a case-by-case basis. But we do not think market failure is pervasive or inherent in our areas of concern.

56/ Note that the mere existence of externalities or other market failures does not by itself provide a sufficient argument for government intervention. There must also be a showing that regulation or other government intervention would improve the situation, at an acceptably low cost.

commission. The judicial approach assumes competition will normally protect consumers' interests, so that government intervention can be limited to (a) occasional structural changes to strengthen competition and (b) after-the-fact penalties and injunctive relief for abuses competition does not prevent. As long as competition in an industry does in fact "work" most of the time, then it seems self-evident that the judicial approach will usually consume fewer public resources than will continuous regulation. And we think it reasonable to assume, unless logic and evidence strongly suggest otherwise in specific instances, that judicial remedies will not impose greater private costs than will administrative regulation.57/

Some remedies currently available help illustrate these points. The common law allocates to the individuals most directly concerned the responsibility to respect the rights of others, as well as the right to seek redress if one's rights are invaded. It is highly empirical, in that it generally takes action only upon presentation of factual evidence that some offense has truly occurred. In particular it does not seek to ban in advance an entire catalogue of hypothetically possible abuses that may or may not be likely to happen. It can be tailored to fit particular situations and relies on incentives directed at the various parties' self-interests. Sometimes the method used is to

57/ These and related issues have been discussed frequently in both the legal and economic literature. See, e.g., A. D. Neale, The Antitrust Laws of the U.S.A., (1960), esp. chaps. 12-15; or Clair Wilcox, Public Policies Toward Business, 4th edition, (1971), passim.

define a property right, for example, in some aspect of privacy. Or often it simply allows an action for damages when someone is injured by the act of another. The principles of the common law are sufficiently broadly conceived to be highly cost-effective in many contexts and applicable to a wide range of circumstances.58/ But where the cost of using the courts is very high, for example because it is difficult to bring reliable evidence to the adjudicative procedure, or in cases where the underlying structure of an issue is changing very rapidly, judicial enforcement of remedies may be less attractive.

Copyright and patent law take a somewhat different approach. Here the entitlement is always protected by a property right. Where transactions are easily arranged, and after-the-fact evaluations of the right uncertain, the law generally requires that use rights be arranged in advance. It is noteworthy that when advance arrangements are hard to make, as in the performance of music, the copyright system becomes complicated to administer and a basis of costly contention between the claimants to royalty revenues.

58/ On this subject, see generally Richard Posner, Economic Analysis of Law, 2d ed., Little Brown, (1977), §8.2 and chap. 13. We follow Posner in classifying as "common law" not only law made purely by judges, but also any statutorily-based judicial enforcement of private rights that has the same evolutionary characteristics as common law.

Regulatory control takes a third approach. Certain forms of behavior may simply be forbidden, perhaps in advance of their ever occurring. Where certain rights are held by society to be inalienable (perhaps in connection with information about individuals), or when the government has a clear cost advantage in controlling behavior, the regulatory approach may constitute a reasonable (or perhaps the best) tack.59/ But it is hampered particularly by inflexibility (consider the unwieldy requirements of the Administrative Procedures Act, which often delay even small rule changes by a year or more), by all the problems of bureaucracy, including often destructive political pressures, and by chronic and serious information problems. Direct control should be a sort of "last resort," only after a strong showing that common law, statutorily-based judicial remedies, and patent- or copyright-like approaches are infeasible or otherwise undesirable.

A final approach is for the government to abstain. The effect of this (non-)policy is to grant everyone a hunting license for information, signals, and the like. Anyone who wishes some degree of information privacy or communications security will have to provide it for himself. Where private provision of security is the least-cost method, and where the costs of using courts and commissions to protect property rights are high, no policy may be the best policy.

59/ For a further discussion of the various rules for protecting entitlements see Guido Calabresi and A. Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 Harvard L. Rev. 1089(1972), esp. section III.

## VIII. An Application of Economics to Remedies

Let us consider alternative remedies for unauthorized intrusion upon a radio system.60/ Such a system might be used to convey point-to-point messages (either for common carriage or for one company's internal data), subscription entertainment services, or other information. Assume a modified version of Section 605 that would offer government protection against unauthorized reception-cum-use of radio signals only when the transmitting parties encrypt or otherwise scramble their signals.61/ We treat two main forms of government action: (1) a statute that allows enforcement of private rights of action through the courts, i.e., lawsuits that would allow plaintiffs to seek damages or injunctions against offenders; and (2) police-like government activities to apprehend offenders and seek criminal penalties against them.62/ Economic analysis can help explain the differing efficiency consequences of these alternative remedies.

60/ We take a radio system to be any wireless communications systems that uses the radio spectrum, including television, data, and voice.

61/ Section 605 of the Communications Act, prohibits unauthorized reception-cum-use (or divulgence) of signals under Federal jurisdiction. It does not distinguish between wireline signals and signals that use the radio spectrum. Our example, however, makes such a distinction implicitly. We would not necessarily apply the arguments of this section to wireline signals.

62/ For purposes of analysis, we discuss these two alternatives as if they were mutually exclusive, although in the real world they might easily be complements.

Perhaps the chief problem with the second alternative is that it probably would not work well unless a government body, like the FCC, set technical standards for acceptable encryption. Absent such standards, transmitting parties would have clear incentives to use cheap methods of encryption, which no doubt could be defeated easily. In effect, the transmitting parties would be seeking to pass to the government as much of the protection costs as possible. So we believe the government would need to set an encryption standard to avoid litigation and "game playing" about what is or is not "encryption." An appropriate and workable standard could then cause profit-making companies to pay reasonable shares of their own protection costs. Such a distribution of cost-sharing will strike most of us as desirable on grounds of simple fairness. And, given the inherent problems of bureaucracies, it will probably lead to an economically more efficient enforcement regime than will a system that relies mostly on government activities simply to round up intruders.

But the standards-setting solution has at least two possible drawbacks: (1) The government body that sets the standards probably will have neither the information, the technical personnel, nor the decisional flexibility of the private sector, so there is a high probability government will select a "wrong" standard. (2) Even if the government selects the correct (i.e., the economically efficient) standard based on today's technology and costs, there is a substantial danger that whatever standard it selects will be set in concrete for

years, despite having been superseded relatively soon by new technical possibilities. Such inflexibilities in technical standards today plague much of U.S. telecommunications policy, in our opinion.

A judicial approach offers promise of a more flexibile and efficient remedy. Assume that our modified Section 605 would allow transmitting parties who encrypt to go before the courts and seek relief against unauthorized reception, but that it would provide no additional government role. Further, it would in no way attempt to define encryption or set technical standards for it. What would then be the results?

We foresee, most importantly, two interrelated outcomes. (1) Firms would have weaker incentives to "play games" with the definitions and levels of encryption.63/ They would be led by the profit motive to get about the business of finding the encryption systems best suited to their own signal characteristics, transmitting technologies, financial positions, and customers. (Note that these factors, especially customers, might vary across the country even for a single service like MDS. Such diversity makes it even more improbable that a Washington-

63/ Attempts to adopt trivial or ineffective encryption systems would probably tend to be self-limiting, insofar as they would force the transmitting firms to spend more and more resources on detecting and suing signal thieves. We think this process would probably lead them to adopt meaningful encryption methods rather soon, as long as they knew a Federal communications police force would not take on the enforcement burden and bail them out.

imposed technical standard would turn out to be the efficient solution.) (2) Firms would simultaneously have incentives to search for the most economic trade-offs between encryption and prosecution. This balancing between encryption and prosecution costs would not occur if responsibilities were split between the private sector and a government "communications police" agency. It is a well-accepted proposition in economics that such internalizations of resource allocation decisions are generally efficiency-increasing and hence are economically desirable, in the absence of complicating factors like scale economies.

Thus economic analysis suggests that, in the absence of important scale economies or externalities, a judicial approach to the protection of encrypted radio signals is likely to be more efficient economically than an administrative, police-like approach. We think the reasoning is equally valid whether signal security is needed in a particular instance for personal privacy, for commercial privacy, or for protection of subscription entertainment service.

## IX. Concluding Thoughts

It is not obvious to us that competitive markets will fail most of the time, or even much of the time, to provide consumers and workers with the "right" amounts of privacy -- i.e., the amounts of privacy they are freely willing to pay for in the form of higher product prices or lower real wages, or in the form of higher taxes. We remain open on a case-

by-case basis, however, to persuasion by logic or strong evidence. At this stage in our research, we have not examined as much of the relevant literature, evidence, and law as we would prefer. But we note with interest that the industries most prominently mentioned in the literature on privacy and most frequently encountered in privacy legislation -- credit, banking, insurance, health, and government -- are either heavily regulated or tend otherwise to have monopolistic characteristics. In telecommunications specifically, we think privacy problems are less likely to arise from failures of competitive markets per se than from the monopoly structures imposed by regulation and other government policies. To evaluate the needs for additional government-imposed privacy safeguards in telecommunications, we suggest addressing the following series of questions: (1) Is the specific concern at issue likely to cause a significant problem in a competitive market? (2) If not, is the relevant market monopolistic or workably competitive? (3) If the market is not workably competitive, can it be made so? (4) For markets or industries where competition is not likely to solve privacy problems (i.e., where there truly are significant market failures), then are continuous regulation or other forms of administrative intervention the best remedies? Or (5) would stronger rights of private action, via the courts, seem to offer solutions at lower total social costs? And (6) for situations where competition-via-deregulation is ruled out by technical or political factors, is more regulation necessarily the answer? Or (7) can stronger rights of private action be usefully superimposed upon existing regulatory systems? Finally, (8) would new

approaches to patent and copyright, like patentability for encryption chips and copyright for encryption algorithms, or other new concepts of property rights in both personal and commercial information, sometimes provide more cost-effective safeguards to privacy than either regulation or private tort actions?

Recent Working Papers & Staff Reports
Office of Plans and Policy
Federal Communications Commission

Divestiture and the Separate Subsidiary Requirement
by Florence O. Setzer, March 1984. Working Paper #11

The Effects of Higher Telephone Prices on Universal Service
by Kenneth Gordon, John Haring, March 1984. Working Paper #10

Measurement of Concentration in Home Video Markets
by Johathan D. Levy and Florence Setzer; December 1982

A Framework For a Decentralized Radio Service
Alex Felker and Kenneth Gordon; September 1983
NTIS # PB84 101609; $10.00; pp. 55

Implementing New Technology in the Land Mobile Radio Service
Philip B. Gieseler; September 1983
NTIS # PB84 101391; $11.50; pp. 80

Statistical Determinants of Radio Stations' Revenues and Trading Prices,
by James A. Brown, Jr., August 1982. Working Paper #9

Deregulation After Divestiture: The Effect of the AT&T Settlement on
Competition, by Daniel Kelley; April 1982. Working Paper #8

Measurement of Concentration in the Home Video Markets
Florence O. Setzer, Jon Levy 1982

UHF Viewing and Channel Selector Type
Steven Brenner and Jonathan Levy; February 1982
NTIS # PB82 177577; $13.50; pp. 133

FCC Policy on Cable Ownership
Kenneth Gordon, Jonathan Levy and Robert Preece; November 1981
NTIS # PB82 140237; $18.00; pp. 217

UHF Reception and Television Preamplifiers
Alex Felker; April 1981
NTIS # PB83 112136; $13.00; pp. 124

Policies for Regulation of Direct Broadcast Satellite
Florence Setzer, Bruce Franca and Nina Cornell; September 1980
NTIS # PB81 151201; $12.50; pp. 131

Comparability for UHF Television: Final Report
Philip Gieseler, Virginia Armstrong, Steven Brenner and Alex Felker
September 1980; NTIS # PB82 218710; $24.00; pp. 275

ABOVE PUBLICATIONS MAY BE ORDERED FROM NTIS BY MAIL OR TELEPHONE. PLEASE INCLUDE NTIS NUMBER (SEE ABOVE) WHEN ORDERING

NTIS
U.S. Department of Commerce
Springfield, VA 22161