Can Markets Generate Privacy in Telecommunications?

by Eli M. Noam

Columbia Institute for Tele-Information
Graduate School of Business
809 Uris Hall
New York, New York 10027
(212) 854 4222

Can Markets Generate Privacy In Telecommunications?

Prof. Eli M. Noam
Professor of Finance and Economics
Director, Columbia Institute of Tele-Information
(212) 854-4596
(212) 932-7816

Can Markets Generate Privacy in Telecommunications?
Prof. Eli Noam

I. Introduction:

Privacy in telecommunications is an issue of growing concern. In the early years of telecommunications, manual operators, party lines, and the absence of a warrant requirement for wiretapping[1] all created their own problems. The first American patent for a voice scrambling device was issued as early as 1881, only five years after the invention of the telephone. There is evidence for telephone wiretaps by private parties and individuals ten years after Bell's patent.[2]

Today, a new generation of privacy problems has emerged. Reasons for this development include:

a) An increasing number of transactions are conducted electronically.[3]

b) It has become easier and cheaper to collect, store, access, match, and redistribute information about transactions and individuals.[4]

c) The number of carriers and service providers has grown enormously, leading to an increasingly open network system in which information about use and user is exchanged across companies.

d) Transmission conduits increasingly include unsecured portions, for example due to mobile communications.

---

[1] Olmstead v. United States, 277 U.S. 438 (1927)

[2] Westin (1967).

[3] For example, in 1962, the U.S. federal government had 1030 computer central processing units; in 1972, 6,731; in 1982, 18,747; and in 1985, over 100,000. (Linowes, 1989)

[4] In the past twenty years the cost of access to a name on a computer-based mailing list has come down to about one thousandth of its earlier cost.

Specifically, there have been recent controversies including: telemarketing and the invasion of privacy in the home; the use of databanks to collect and redistribute personal data; the ability to determine a caller's phone number prior to accepting the call using Caller ID services and the re-use of such information, and; the ability of employers to use intra-organizational networks to monitor their employees.

Concern with electronic privacy has led to different policy approaches. Western European countries, for example, have passed comprehensive (omnibus) data protection laws and established institutionalized boards and commissions which have often imposed fairly rigorous restrictions on information collection and data flows.[5] In the US, the approach has been less systematic, resulting in a variety of ad hoc federal and state legislation. These laws, as they relate to telecommunications, have usually been established outside the state public utility commissions or the FCC, and they often addressed only a specific issue of concern.[6] Most of these statutes are either aimed at other industries (for example, credit rating bureaus), or at conduct of governmental agencies, or they deal with flagrant abuse such as computer break-ins.

In the past several years, several state utility commissions have dealt with the Caller ID issue. The New York PSC, in particular, went beyond a problem-specific approach to privacy protection, and issued, after a proceeding initiated by the author, a set of broad privacy principles applicable to a whole range of telecommunications services.

---

[5] See Eli M. Noam, Telecommunications in Europe, Vol. I, Oxford University Press, 1993.

[6] A 1990 example is a Congressional bill for monitoring of computer bulletin boards by the host system operators in order to prevent use for illegal activities.

The regulatory approach, however, is not the only way for society to deal with privacy problems. Another approach would be to rely on market forces to provide the optimal amount of privacy protection. But would this approach work? It is impossible to answer this question without a more thorough analysis. For certain privacy problems it might, while for others it might not.

This paper will, therefore, analyze the potential for market based responses to the privacy threats that are emerging with the rapid evolution of telecommunications technology and network market structure. It will attempt to identify when the market can and cannot be relied upon to resolve various privacy issues, and where a regulatory response will be necessary.

II. Background:

What is privacy? In the telecommunications sector, privacy consists of two distinguishable but related aspects:[7]

(a) The protection against intrusion by unwanted information. This is sometimes termed "the right to be left alone,"[8] and it is an analogue to the constitutional protection to be secure in one's home against intrusion by government.

(b) The ability to control information about oneself and one's activities; this is related in some ways to proprietary protection accorded to other forms of information through copyright laws.[9] A related aspect is the security of information about oneself from tampering by others.

---

[7] See, e.g., Richard Posner, (1981).

[8] Warren and Brandeis, (1890).

[9] The common-law copyright protection provided primarily that if one had not published information in one's possession, no one else could take and publish it. This was similar to a trespass and conversion action.

The common aspect of both these elements is that they establish a barrier to informational flows between the individual and society at large. In the first case, it is a barrier against informational inflows; in the second instance, against informational outflows.

The concept of privacy is not without its detractors. There are three major criticisms:

(a) "Privacy protects anti-social behavior"

To the contrary, privacy is one of the touch-stones of a civilized and free society.[10] Authoritarian or backward societies do not value a private sphere since they rarely respect individuality and subordinate it to the demands of rulers or social groups.[11]

(b) "Privacy is costly to the economy"

Privacy protections raise the cost of information search. Potential employers and buyers, for example, have to spend more effort and money to find out who they are dealing with if access to personal information is restricted. Deception becomes easier and transaction costs rise.

But there are also good economic arguments in favor of privacy. It affects the ability of companies and organizations to hold on to their trade secrets and details of their operations, and to protect themselves from leaks of insider information and against

---

[10] Justice Louis Brandeis, in a famous dissent, wrote of "the right to be left alone -- the most comprehensive of rights and the right most valued by civilized men." Olmstead v. U.S., 277 U.S. 438, at 478 (1927).

[11] On the history of privacy, see Posner (1981); Simmel (1906); Westin (1965); Seipp (1978). In the United States, privacy is a non-partisan issue. The Privacy Act of 1974 was co-sponsored by Senators Edward Kennedy and Barry Goldwater.

governmental intrusion. Information often has actual value, and since much of it has no protection through property rights, it must be protected through confidentiality or secrecy.[12] To permit its easy breach[13] would lead to a lesser production of such information. It has been shown in a theorem by Greenawalt and Noam (1979) that under normal conditions "information of value, once released to one person (or very few persons at most) will spread -- in the absence of collusion -- to all participants." Hence, the absence of privacy protection to stem outflow of information will lead to suboptimal production of such information.

Similarly, anonymity may increase economic risk-taking (though increase it for their partners to a transaction); certain investments may be curtailed if the identity of their investors were disclosed. In that sense, privacy protection acts as a spur to investment, just as the protection of limited liability offered to corporations. (Of course, illegal activities are also made easier.)

The loss of privacy also leads to inefficiency in information flows, just as excessive privacy protection may. In the absence of privacy, people use all kinds of hints or codes in order to reduce the outflow of information. Or they may meet face-to-face instead of using the telephone.

---

[12] In the extreme, private information is so valuable to an individual as to make him a target for blackmail. See also Brown and Gordon (1980) for an economic perspective from the FCC.

[13] In an information-based society and economy, the incentives to acquire information are continuously increasing. See Posner, (1981, pp. 231-347), as the most comprehensive discussion of the economics of privacy.

Partly in response to economic and social needs, many transactions have been specifically accorded special informational protection known as "privileges," e.g. between attorney-client, penitent-clergy, patient-doctor, citizen-census taker, etc. The idea in each case is that the protection of information leads to a socially superior result even if it is inconvenient in an individual instance to others.

(c) "There is no demand for Privacy"

To the contrary, attention to privacy is widely shared. For example, according to information from the New York Telephone Co., 34% of all residential households in Manhattan and 24% of all its residential households in the State have unpublished telephone numbers at subscribers' request. Most policemen, doctors, or judges, to name but a few professions, have unlisted numbers. On the West Coast, it appears that the spread of unlisting is still further advanced, reaching 55% in California![14]

---

[14] Another indication is provided by a survey conducted by the American Express Co. among its card holders. 90% felt that mailing list practices were inadequately disclosed, 80% that information should not be given to a third party without permission, and more than 30% believed federal legislation was needed to restrict the use of lists. "Privacy Study Reveals lack of Consumer Confidence," Direct Marketing, Dec. 1988, p. 8, in McManus (1989). It should be noted that American Express makes extensive use of the data that it has accumulated on its cardholders. According to Fortune, the company computers "maintain and update weekly a profile of 450 attributes--such as age, sex, and purchasing patterns--on every cardholder." (Newpert 1989, p. 82.)
A 1988 survey by the Massachusetts Executive Office of Consumer Affairs of the main consumer complaints found them topped by telemarketing and promotional mailings. Kathryn Marchocki: "Prize letters, phone spiels top list of consumer beefs," The Boston Herald, Jan. 5, 1989, p. 47; in McManus, (1989), p. 47. Pacific Bell planned in 1986 to sell subscribers information such as new phone orders; more than 75,000 complaints came in,

III. How Do Market Transactions Affect Privacy?

A framework for analysis is the theorem of Nobel Prize winning economist, Ronald Coase. In his article, The Problem of Social Cost[15] Coase argues that a conflict in the rights of two people the final outcome will be determined by economic calculus and (assuming low transaction costs) result in the same outcome regardless of the rule of law.

Coase does not argue what should be, he argues what will be: "the question is commonly though of as one in which A inflicts harm on B and what has to be decided is, How should we restrain A? But this is wrong. We are dealing with a problem of a reciprocal nature. To avoid the harm to B would be to inflict harm on A. The real question that has to be decided is, Should A be allowed to harm B or should B be allowed to harm A? The problem is to avoid the more serious harm." Ronald Coase, The Problem of Social Cost, p. 96.

Applied to privacy in telecommunications, this suggests that the distribution of rights may have little impact on the final determination of what will occur. For example. whether or not a private person has a "right" to exclude telemarketers from calling their home, or whether the telemarketers have a "right" to initiate phone calls at their pleasure may not be conclusive in regards to whether or not such a telephone call actually takes place. The difference will be which party must pay the other party in order to obtain agreement to waive their rights. This makes a difference to wealth distribution, but to whether the call is made.

Let us use an example: A homeowner prefers not to be called by telemarketers. But, the telemarketer needs to contact people at

---

and the company backed off."Pac Bell backs-off selling lists," Alameda Times Star, Apr. 16, 1986, p. 16, as cited in McManus, (1989).

[15]The Journal of Law and Economics 3 (October 1960): 1-44.

home in order to generate business.

While such a conflict in rights (the right to be left alone in one's home versus the right to solicit business using the telephone) could be resolved through legislation. Exchange transactions may also resolve the problem.

Both of the parties attribute a certain utility to their preference. For example, it may be worth $3 to the salesman for the opportunity to talk to me on the phone. If necessary, he would be willing to offer us this money for the opportunity to persuade me.

Now imagine that I would be willing to pay the salesman $4 to keep him off the phone. The $4 is the value I place on my privacy in that instance. If the salesman has a **legal right** to call me at home, I would "bribe" him not to call me.

The regulatory rule may be either to prohibit unsolicited calls, or to permit them, but regardless of which rule is adopted, the call will not take place, because the value, to me, of my privacy is greater than its interruption is to the salesman. Conversely, if for some reason the value to him would rise, say to six dollars, he would make the call, and if necessary buy my cooperation.

In other words, the distribution of the legal rights involved (what is illegal and what isn't) only determined who had to bribe whom. The law did not necessarily determine whether the telemarketing call actually took place, it only determined the final wealth distribution.

Important factors that can interfere with this ability of two people to negotiate are transaction costs. For example, the inconvenience to negotiate a calling price could exceed the value of the telephone call for either of us. Laws should be designed to distribute rights in such a way as to reduce transaction costs. In this way, the reduction in transaction costs increases the possibility that the parties involved in a conflict will agree on

an efficient resolution, and do so in a cost-minimizing fashion.

To deal with transaction costs, Coase suggests that if the telemarketer has a right to call a customer at home then the homeowner will have to track down the telemarketer and bribe him to not make the phone call. If, on the other hand, the telemarketer does not have a right to call a customer at home then the telemarketer has to bribe the homeowner to get the homeowner's permission to call. As discussed above, this is a significant transaction cost. The transaction costs are most likely lower in the second situation, especially if technology provides a solution.

A second and serious outcome is know as the moral hazard problem. A moral hazard is any condition that encourages a party to act inefficiently. In the above example, a situation in which homeowners would have to bribe telemarketers to keep them off the phone would be a clear moral hazard. Telemarketers would have the incentive to threaten to call the same homeowner hundreds of times each day just to get paid to go away. In effect, they would cease being in the business of selling, and instead be in the business of selling protection from their own interference.

This would be the case where the cost (including in terms of reputation) to telemarketers to initiate calls would be low relative to the nuisance value to the consumer. This moral hazard factor suggests that the right of exclusion should be assigned to the consumer if markets are to function efficiently. Thus gets us to the next question, how such a market might realistically function. Therefore, legislators, courts and regulators must take moral hazards into account when distributing rights.

In the future, Telecom equipment or service providers might offer equipment for customers that will allows them to select among their incoming calls electronically those calls they want to be compensated for. Such a service might be described as **Personal-Service**. The service would block incoming telephone calls to a consumer with an electronic message and a series of options. Upon

placing a call, the caller would be informed that the customer "charges" telemarketers for the privilege of speaking to them.

Individual customers could set different price schedules for themselves based on their privacy value, and even the time of day. The incoming caller would be informed that if he or she is a telemarketer and is willing to pay for the privilege of speaking to the customer they should proceed. By proceeding, the telemarketer enters into a contractual agreement. The telecom service provider would then automatically handle the billing by shifting money between the accounts (e.g. a telephone bill or credit card account) in question. Under this system the problem of telemarketers would be handled by mutual contracts rather than through regulation.

Such a system will have a negative impact on the business of telemarketers. Currently, they "externalize" some of their costs by utilizing the telephone to get the attention of potential customers. Under personal-900, telemarketers will be forced to pay the true cost of obtaining consumer attention.

Consumers, too, will end up paying at least some of the portion of these costs by way of higher prices. The extent to which these costs can be shifted to buyers depends on the relative elasticity of demand and supply.

Some consumers will benefit, do the payment they receive for the call. Others might even become "professional call-receivers," though telemarketers may devise ways to select the most likely buyers.

It is also likely that high income consumers who value their time at a higher rate and who are more desirable to telemarketers will, therefore, charge telemarketers more for each call.

CALLER IDENTIFICATION:

Caller ID technology has become the focus of much debate about privacy. This service provides the called party with the directory number of the calling party and enhances the privacy of called recipients because it allows them to identify the caller in

advance. However, opponents assert that Caller ID violates the privacy rights of the caller by disclosing their telephone number and making possible their inclusion into mailing lists. This dilemma creates a conflict in privacy desires. A market based solution would likely involve both the opportunity of subscribing to caller I.D. and the opportunity to "block" one's telephone number from such services.

Before discussing the possibility of offering both conflicting services we need to analyze the role "competition" plays in a market based solution to privacy problems. Under the Coase Theorem, competition is not a mandatory part of an efficient solution. That's because the theorem argues that if a solution exists that is desirable (creates a profit) for both sides (and is, therefore, more efficient) then a monopolistic player will be just as willing as a player in a competitive environment to consent to the solution.

A monopolistic situation does create some interferences to a Coasian solution. First, monopolists are not obligate to bargain efficiently. Monopolists can demand "bribes" that are much larger than would be necessary in a competitive environment. Monopolists cannot, however, demand bribes that are so large that the solution becomes undesirable for the non-monopolistic party.

An example of this can be found in the situation involving the telemarketer and the consumer. Let's make the consumer a monopolistic player -- the only person who could possibly want to purchase the telemarketer's product. The telemarketer must make a sell to this operation or else he won't make a sale at all. If the consumer is aware of this fact, the consumer can demand a larger payment for the telephone call than normally be required.

But the consumer cannot demand a price that's greater than the value the telemarketer places on the call. Such a demand would make the deal unprofitable for the telemarketer and, therefore, the call would not be made and neither party would make a profit.

The second affect monopolists have on a Coasian analysis is they can reduce the number of different arrangements that could be profitable for two parties. An example of this problem can be found by returning to the controversy involving "Caller Identification.

Currently, Local Service Providers want to offer Caller I.D. to customers because they can serve some customers and make a profit in doing so. At the same time, they expose the privacy of unwilling callers. Yet the Local Service Providers do not want to offer "Caller I.D. Blocking" as a service because the profits that could be made off this second service will be less than the loss in profits that will be incurred upon the Caller I.D. services. (Once a lot of people start blocking their numbers from Caller I.D. machines the value of these machines will be much less and people will be less willing to buy them.)

In a competitive market this problem of conflicting services would solve itself. While offering "Caller I.D. Blocking" might be unprofitable for the Local Service Provider that is also marketing Caller I.D., it would not be unprofitable for as competing company that is not enjoying Caller I.D. profits. Therefore, in a competitive market "Caller I.D. Blocking" would be offered by other companies as a solution to the second privacy problem. Both services would probably reduce each other's market (once people reduce buying Caller I.D., people will also reduce buying "Caller I.D. Blocking"), but the end result will be that two market based solutions resolved specific privacy problems, though at a non-neutral distributive impact.

Wireless Transmission:

Market transaction would succeed in preventing electronic eavesdropping to cellular and cordless telephones. For example, Cellular service providers or equipment firms could offer "scrambling" devices for an additional fee. Customers sufficiently

interested in privacy would purchase or lease the scramblers. Cellular firms could also compete by offering scrambling.

While such privacy schemes may require less efficient use of spectrum, companies are already developing such security equipment, because they respond to user demand. In 1991 GTE Mobilnet released a encryption system packaged for the cellular-consumer market.

GTE Mobilnet developed the system because some customers -- mostly government accounts and defense contractors -- were concerned about the illegal use of scanners that can monitor radio waves over which mobile-telephone signals move, allowing them to listen to others' conversations.[16]

IV. MARKET PROBLEMS:

While the market may provide efficient solutions to privacy issue in many instances, it will not always work. In some cases significant transaction costs will interfere with a resolution to a privacy issue even if the resolution is valued by all the parties involved. A regulatory response can reduce the transaction costs in some instances, but not in every case.

DISCLOSURE LAWS:

At this point it should be noted that "regulation" or "legislation" does not always mean a wholesale redistribution of rights. Instead, legislatures can intervene in some situations by passing laws that eliminate specific transaction costs, rather than alter the entire balance of power in a negotiating situation.

A prime example of such "tinkering" with transaction costs is legislation requiring that any company which receives information

---

[16]The device, which is about the size of a pocket calculator, will work for installed car and transportable cellular phones -- but not handheld mobile telephones. It can easily be installed by customers between a mobile telephone's handset and the transceiver. GTE MOBILNET OFFERS NEW SERVICE THAT ALLOWS MOBILE-TELEPHONE CUSTOMERS TO SCRAMBLE CONVERSATIONS, Copyright 1991 PR Newswire Association, Inc., May 16, 1991

about an individual or other company must **disclose** to that person or company exactly what will be done with the information. If the recipient of private information plans to sell it to other companies, the recipient most notify individuals **in advance** of the receipt of the information. If the company plans to use the information in order to design directly mailings or telemarketing campaigns, this information must be disclosed also. Any purposes that are not disclosed cannot be applied to a specific piece of data.

A disclosure law such as this would enable consumers to know where information about them is going and what it will be used for. This will enhance their ability to decide how they will respond to the prospect.

DATA BANKS:

In other situations, simply "tinkering" with transaction costs may be insufficient to compensate for enormous obstacles to successful negotiating. An example of such "market failures" can be found in the collection of and transfer of "data bank" information. These data banks include statistics on people's financial and medical health, criminal record and even personal and political preferences.

Currently, companies can sell information about their customers to "credit agencies" which, in turn, sell the information for a variety of purposes. Insurance companies want to know the medical history about new applicants; stores want to know if new customers are credit-worthy; employers want to know if job applicants have criminal histories; landlords want to learn if a potential tenant has ever filed a complaint against a former landlord; and doctors want to know if a patient has brought a malpractice suit against another doctor.

"Horror stories about the misuse of information are surfacing. The Privacy Journal recently published a collection of stories about 200 individuals who lost their jobs or suffered in other ways

because incorrect information had been collected about them. In one instance, a man was fired from his job when his employer unearthed a false report that said the man had been convicted of a drug-related crime."

"Thanks to technology, the consumer information business has grown into a more than $ 1 billion-a-year business. Three of the United States' largest credit bureaus, Equifax, TRW, and Trans Union, thrive on the sale of information from the hundreds of millions of records they have collected. Equifax alone reached $ 1 billion in revenues last year."[17]

Companies have a legal right to collect and redistribute personal and financial data about individuals. Consumers also have the right to offer companies "bribes" in an effort to get them to stop, but the transaction costs, along with the bribery costs are high.

First, right now consumers have no way of knowing what companies have personal data about them and what is being done with that information. As explained above, disclosure laws could alleviate this problem.

Secondly, consumers would probably be unable to bribe **every** holder of personal data about them, plus bribe everyone that potentially could hold personal data about them. This phenomena can be called **the rule of gossip**. Put simply, information can be reproduced and distributed so easily that it is nearly impossible to contain data once it is in the possession of a single third party. The holder of personal data can easily "publish" the data in such a way that literally thousands of information collectors can possess and utilize the material. This possibility is

---

[17] Susan E. Fisher, What do computers know about you? Personal information too readily available; Includes related articles on privacy issues and US right to privacy laws, PC Week Copyright (c) 1991 Information Access Company; Vol. 8; No. 6; Pg. 156, February 11, 1991

evidenced by the status quo. The average person is on 100 mailing lists and 50 databases at one time.[18] It would be nearly impossible for an individual to locate and bribe everyone who has access to the information intended to be contained.

The increase in the price of the information, however, probably would not increase at the same rate as the increase in the number of participants. Suppose the exclusive control of a piece of information yields its holder a special profit P; and suppose for the moment that the size of the benefit, if shared by several people, will still remain the same, but that it will be divided, but that it will be divided among all the holders. For example, in the individual share for two owners will be P/2, for three owners P/3, and so on. Thus, the individual profit from the information will diminish and approach zero as the number of holders becomes large.[19]

A moral hazard would also exist. Companies that never planned to utilize personal information could threaten to do so just to get the bribes. Consumers could attempt to respond to this problem by trying to stop data from getting released to a third party in the first place. For example, people could refuse to do business with, and reveal information to any company that does not agree to destroy the personal data immediately following the completion of the transaction in question.

With an automobile dealer such an agreement when mean

---

[18]Robert Ellis Smith, publisher of Privacy Journal, in Providence, R.I." Susan E. Fisher, What do computers know about you? Personal information too readily available; Includes related articles on privacy issues and US right to privacy laws, PC Week Copyright (c) 1991 Information Access Company; Vol. 8; No. 6; Pg. 156, February 11, 1991

[19] Eli Noam & Kent Greenawalt, Confidentiality Claims of Business Organizations, in Business Disclosure: Government's Need to Know, Harvey J. Goldschmidt, ed., p. 400

promising not to transfer auto-loan information to other companies and to destroy the loan information once the loan is repaid. For a video rental dealership, the agreement would mean destroying any record of what movie was rented by a person once the movie was returned to the store.

Companies interested in improving their public image could advertise that they always agree to limit the use of information to single transactions. Some exclusive mail order companies in the United States already do something along these lines (they advertise that they never sell to other companies their mailing lists).

Of course, companies would have to charge customers higher prices to compensate for the agreement. These higher prices would be necessary for three reasons. First, companies would need to compensate for the income lost be agreeing to stop selling information. Secondly, once a lot of companies start refusing to sell information data on individuals will become more scarce and, therefore, more expensive to purchase.

Finally, companies that refuse to pay the increased costs of information will lose larger sums of money dealing with customers without first obtaining background data on them. This is because the companies will no longer have the information necessary to avoid dealing with high risk customers. The increased exposure to high risk customers will increase default rates and, subsequently, the costs of doing business.

The added expenses that are created, however, could be passed onto to customers. In this manner, customers can "purchase" the ability to prevent information about them from become a "product" on the open market.

The major problem with this approach is that it will only work in regards to transactions between individuals and businesses. Where an individual is not involved (perhaps because the information was obtained from a public record, or through illegal

means) no market based incentive exists to prevent transfer of the data.

An "attempted" Coasian solution to this problem is to redistribute the rights involved in the arrangement. Currently, companies have a right to collect, distribute, and utilize personal data about individuals. What if the roles were reversed and companies had to get a person's permission before they could retain, transfer or utilize personal data?

Under this second distribution of rights companies that depend on the use of personal data (e.g.: banks considering the advisability of issuing a loan) would have to get the persons permission before utilizing data about them. While a loan applicant would probably be willing to allow the use of such information for the loan review without charging the bank for the privilege of such use, a loan applicant would probably want some compensation if the bank wanted to "sell" the personal data to its credit card division looking to design a direct mailing of credit card applications.

As in the telemarketing example above, individuals would be able to set a price for the privilege of utilizing data about them. Schedules of fees could be included on the same documents that contain the personal data in question. Payments could be credited to electronic bank accounts.

Of course, this alternative includes significant transaction costs. One of the biggest obstacles is that consumers will have to police companies to make certain that they do not utilize information without first making compensation. (The expenses of such policing is a valid transaction cost.) This difficulty could be dealt with, however, perhaps with the assistance of a new type of service provider.

For a small fee a company well placed in the computer and information industry could continually run "key word" searches in order to see if a person's name and personal data is utilize for

any un-compensated purpose. (Legislation may be required to provide such companies access to the internal data bases of companies for this limited purpose.) These special service providers could also handle billing and account services for consumers who contract for the services they provide.

V. Intra-organizational networks:

Intra-organizational networks also create the potential for particularly serious privacy problems. The owners of such networks possess the capability to track employee calls, their physical presence, and location, and productivity (e.g., number of key-strokes, call handling time, total time on phone, etc.). The networks also permit eavesdropping on conversations without notification to employees as well as non-employee third parties.

Reports of such incidents are easy to locate. Some industries, such as the airlines, mail order houses and telecommunications companies, electronically monitor their workers to assess their speed, accuracy and courtesy in dealing with customers over the telephone. Some labor unions are pressing for federal legislation requiring employers to notify workers when monitoring occurs and to protect the privacy of data obtained in the monitoring process.

The employer's ability to access employee communications on corporate electronic mail systems is another privacy issue. Employees have sued employers who, they claim, have invaded their privacy by monitoring their electronic mail messages. To date, the courts have supported employers' rights under statute to monitor private electronic mail systems.[20]

Employees could refuse to work for employers which have a

---

[20] Janlori Goldman*, Where the public draws the line; Consumers are learning they can say 'no' to invasions of privacy, Computerworld, Copyright 1991 IDG Communications, Inc., April 15, 1991

reputation of eavesdropping on employees, but more likely such a problem will have to be regulated. This is because employees do not usually have a great deal of ability to transfer from one job to another at will.

Aside from the general scarcity in adequate employment, employees are trapped by several types of transaction costs. These include the difficulty of locating a new job while working in an existing position, the loss of "invested income" such as pensions, seniority, unique training, and accumulated leave time. Finally, a great deal of social pressure exists encouraging people not to change employers frequent.

Because of these high transaction costs, the market will fail in its efforts to solve privacy problems in intra-organizational networks. Therefore, regulation will be necessary to resolve these problems.

CONCLUSION:

The essential element involved in solving future telecommunications privacy issues is reducing transaction costs sufficiently for market based solutions to intervene. As discussed above, in many situations transaction costs make efficient market solutions prohibitively expensive. In some of these cases there is a role for regulators and courts may need to redistribute rights in order to lower transaction costs. In other situations minor legislative efforts such as disclosure laws may correct transaction costs.

The most important thing to recognize, however, is that where transaction costs are diminished new companies and new technologies often provide solutions to privacy problems. So long as people value privacy, service providers will try to find ways to cash in on that value by developing a product and service that satisfies the desires of the consuming public.