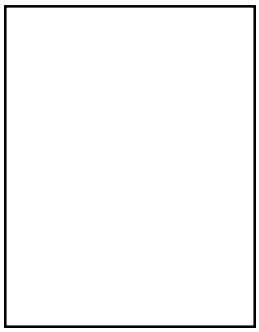
Privacy in Telecommunications: Markets, Rights, and Regulations

Part III: Markets in Privacy

Eli M. Noam, Ph.D.



Dr. Eli M. Noam is Professor of Finance and Economics at Columbia University Graduate School of Business and Director of the Columbia Institute of Tele-Information. He has also served as Public Service Commissioner engaged in the telecommunications and energy regulation of new York State. His publications include over 200 articles on domestic and international telecommunications, television, information, and regulation subjects. He served as a board member for the federal government's FTS-2000 telephone network of the IRS' computer modernization project, and of the National Computer Lab.

Dr. Noam received an A.B., a Ph.D. in economics, and a J.D. law degree from Harvard University.

This article is reprinted with permission from a monograph written by Dr. Noam and edited by Rev. Everett C. Parker of the United Church of Christ. This third and final installment discusses markets in privacy, including a discussion of approaches to ensure privacy.—Ed.

So far, we have discussed statutory and regulatory approaches to privacy problems. But there are other options.

First, there is the possibility of self-regulation, where an industry agrees to restrict itself. Realistically, though, self-regulation is rarely voluntary. It usually occurs only under the threat of government action, and can therefore be considered merely a variant of direct regulation.

As mentioned before, for the state to control and protect privacy is a natural response in the telecommunications field, given its history as a state-controlled monopoly. It has led to a view of privacy problems largely as a static issue of "rights." Such a view is appropriate in the context of political rights of the individual against the state. But the same cannot be said for the privacy claims of individuals against other individuals. Here, the allocation of rights is only the beginning of more complex interaction. Some people may want and need more privacy than others. Privacy, by definition, is an interaction, in which the informational rights of different parties collide. Different parties have different preferences on "information permeability" and need a way to synchronize these preferences, so they will not be at tension with each other. This would suggest that interactive negotiation over privacy would have a place in establishing and protecting privacy, either as a substitute or a complement to direct regulation.

How should one analyze the process of private bargaining over privacy? It is useful to consider as a framework for discussion the economic theorem of Nobel laureate Ronald Coase. In his classic article, "The Problem of Social Cost," Coase argues that in a conflict between the preferences of two people, the final outcome will be determined by economic calculus and (assuming reasonably low transaction costs) result in the same outcome *regardless* of the allocation of rights.[1] If the final result is the same, who then

1070-3683/95/$3

should have the rights? According to Coase, it should be the "least cost avoider," i.e., the party who can resolve the conflict at the lowest possible cost.

Coase does not argue normatively what should be, but rather positively what will be: "The question is commonly thought 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."[2]

Let us apply this affirmation to privacy issues among two private parties, using the example of telemarketing. Both of the parties to a telephone solicitation call attribute a certain utility to their preference. For example, it may be worth $3 to the telemarketer to have an opportunity to talk to the consumer. If necessary, she would be willing to offer a potential customer up to that amount.

Conversely, the consumer would be willing to pay—grudgingly to be sure—up to, say, $4 to the telemarketer to keep her off the phone. The $4 is the value he places on his privacy in this instance. Thus, if the telemarketer has a legal right to call him at home, he would "bribe" her not to call, in order to keep his peace and quiet.

The basic decision on regulatory rights is either to prohibit unsolicited telemarketing calls, or to permit them. But regardless of which rule is adopted, the call will not take place, because under our numerical example, the value of privacy to the consumer is greater than its interruption is to the telemarketer. But if for some reason the value to the telemarketer would rise, say to $6, the consumer could not pay her enough not to call; and conversely, if the telemarketer would have no initial right to make unsolicited calls, she would pay for the consumer's cooperation by a payment of $4 or more, so that the call is welcomed.

In other words, the distribution of the legal rights involved may largely determine who has to pay whom, not whether something will happen. Thus, the law does not necessarily determine whether telemarketing calls actually take place; it only affects the final wealth distribution. this interactive concept is often difficult to grasp if one is used to thinking in absolutes of black-letter law, or if one transposes constitutional principles protecting individuals against the state to person-to-person protections. Common law, in contrast, has recognized transactions from the beginning. Indeed, the original legal cases which established the tort of privacy were not based on a finding that the plaintiff had a right to privacy, but instead that the plaintiff had a right to be adequately compensated.[3] The early cases developing the tort of privacy often involved the use of a person's likeness in commercial advertising without permission or offer of monetary compensation.

For privacy transactions to occur, however, there are several prerequisites. These include:

- Sufficiently low transaction costs.
- A legal environment that permits transactions to be carried out.
- An industry structure that permits transactions to occur.
- Symmetry of information among the transacting parties.
- No "market failure."

Transaction Costs

For exchanges to take place in the market, it is necessary that transaction costs for the parties involved be lower than the benefits from the transaction. Transactions involve a number of obstacles, such as identifying and contacting parties, negotiating, carrying out agreements and enforcing them. Nobody will spend much time and money for a small benefit.

The relevance of transaction costs becomes apparent if we look at the earlier example. In that case, it was worth $3 to the telemarketer for the opportunity to talk to the consumer on the phone, and $4 to the consumer to be left alone. Once its costs are included, however, a transaction may become more difficult. Let us assume the cost to a consumer to enter into an agreement with a telemarketer and enforce it is $3. Given the $4 limit on his preference, he would have only $1 left to offer as the actual price (4 - 3)—not enough to satisfy the telemarketer's own $3 minimum price. Thus, the transaction cost has prevented an exchange. Conversely, if transaction costs for the telemarketer to obtain consent are $1, she would have $2 (3 - 1) left to buy access from the consumer. Yet, at such a price, the consumer would not sell. In other words, in this situation, the initial distribution of the access rights made a difference in the final outcome in that transaction cost prevented an exchange, keeping the outcome at the respective original distribution.

The existence of transaction costs gives Coase a criterion to decide where rights should be allocated,

given that the outcome, as he argues, will be the same absent transaction costs. He advocates a process that would distribute rights in such a way as to keep transaction costs to a minimum. His logic is that the lower the transaction costs are, the fewer resources would be used just in the process of exchange. In so doing, he considers only economic efficiency, but not the impact on the distribution of wealth.[4]

Redistributing legal rights, however, is not the only way to reduce transaction costs. Technology can be employed for that purpose. Third parties could intervene if they are capable of reducing transaction costs sufficiently. This will be discussed further below.

Industry Structure

It makes a difference whether the underlying market structure is competitive or not. A monopolistic market can influence market-based privacy in several different ways. The first impact is an imbalance in the negotiating situation. Monopolists can extract more from the other party than they would in a competitive environment. Monopolists cannot, however, demand payments larger than the maximum (reservation) price of the other party.

In our telemarketing example, if there is only one consumer for a competitive telemarketer's product, he could demand a larger payment for accepting the telephone call than would normally be required—the full $4. Where many consumers exist, they are likely to drive the price down toward $3. Analogously, if a telemarketer is a monopolist and if it must pay consumers an access charge, it will pay only the lowest amount necessary.

Suppose now that there is a carrier connecting A and B. Such a carrier could serve as a transaction facilitator or arbitrageur in privacy and access. It could, for example, offer blocking services for privacy protection where telemarketers have a right to call. Alternatively, if the legal rule is that telemarketers have no right to call, the carrier could offer an "access charge payment service" to telemarketers and help obtain the permission of the residential customers to legally receive marketing calls. The response depends again on the market structure. If, for reasons of technology or transaction costs, only a carrier can provide such services and if such a carrier is a profit-maximizing monopolist, the carrier would supply, depending on the legal rule, a blocking or an access payment technology, and charge for them almost up to the respective reservation prices. For example, it could demand $4 for the consumer blocking, or $3 for the access charge services to the telemarketer, if she needs to buy access. Of the latter charge, some would have to be passed on to the consumer, and it will not be enough, i.e., it will be less than the $4 necessary. But if the value of the call to the telemarketer is $6, then the carrier would extract that amount, and pass on $4 to the consumer for his cooperation. In either case, therefore, the carrier would profit, and in the process generate a market-clearing privacy.

Symmetry of Information

For efficient markets to exist, the parties to a transaction must have information to judge the value of a transaction to them. Yet, a consumer rarely knows what companies plan to do with information they obtain about him or her in a transaction. For example, the provider of an "800" automatic collect-call service about snow conditions may be in the practice of selling the names and addresses to its callers to sports magazines, mail-order marketers of ski equipment, and to travel agents. such practices will be objectionable to at least some callers, particularly when it comes to more sensitive personal preferences. Yet, in most cases, callers have no way of knowing the information-resale intentions of the party they call.

The consequence is that customers may be unable to participate efficiently in a market for privacy protection. This suggests the importance of full disclosure. Organizations which systematically resell individualized information from their transactions need to reveal their policy.

Such disclosure requirements would be similar to those for hazardous and toxic chemicals in the workplace. Congress passed laws requiring employers to notify employees of the existence and propensity of any chemicals utilized in a business or factory. Supporters of the requirements believe that once employees were aware of the dangers that exist in their places of work, they would be able to seek employment with safe working conditions, or additional compensation as incentive for accepting the dangers.

It might be asked whether markets would not generate such disclosure by themselves. While companies have no incentive to make known practices which customers would find negative or worthy of compensation, their competitors could stress their own protection of privacy and contrast it with their rivals' inadequate record. Yet, the experience in securities markets, where firms rarely compete by alerting buyers that they offer more information than their rivals, suggests that there is no great likelihood that this will

work in practice, though it should not be discarded as a possibility.[5] More likely, third party information providers would emerge to alert consumers of potential privacy problems with certain products and services.

Market Failure

A market failure occurs when markets create increasingly inefficient results, and where transactions do not take place as a result. One market failure situation is the creation of disincentives to efficient behavior. Such a "moral hazard," as economists call it, would occur in the telemarketing example if customers would have to pay telemarketers to keep them off the phone. In such a situation, a telemarketer would have the incentive to call the same customer repeatedly, possibly under varying identities, just to get paid to go away. Other telemarketers would emerge for the purpose of collecting such fees. In effect, they would cease being in the business of selling merchandise, and would instead be in the business of selling protection from their own interference.[6] The market wouldn't result in equilibrium; to the contrary, it would be unstable, with a more-than-ever number of calls reaching a less-than-ever well-off consumer. Yet, this moral hazard factor does not prove, by itself, that a market will not work. It suggests simply that the right of exclusion should be assigned in this case to the consumer.

Another type of market failure is created by the "public good" nature of information, which permits "free riders." A free rider can benefit from information without having to compensate the owner of the information. Unlike most types of property that are private, information has some of the characteristics of a "public" good: it can be used by more than one person at the same time with no harm to other users, and it may not be possible to exclude other parties. If free riders cannot be excluded from benefiting from the information, no one would ordinarily pay enough for it to make its dissemination or even production worthwhile, and no trading in information would occur. For that reason, the holder of information will try, through secrecy and selective selling of the information, to maintain as much as possible its "private" character.[7]

Another market failure can be caused by negative externalities, i.e., when a portion of the costs of an activity are borne by a party who is not benefited by the activity. An example is a factory which pollutes the air. The pollution is a cost of the operation which is borne by everyone in the community. Because the firm does not have to pay for the damage caused by the pollution, its operations seem to be more profitable than they are, and economically incorrect incentives to keep the operation exist. (The Coase transaction analysis breaks down when the number of affected parties is large.)

Freedom to Transact

Another prerequisite to privacy transactions is a legal system which permits them or at least does not establish incentives in the opposite direction. While free transactions would lead to the offer of services that reduce privacy, the opposite tendency is just as likely if consumers care for privacy. Take, for example, the traditional profit regulation of telephone carriers, known as rate-of-return regulation, as contrasted to the regulation of prices. Since a carrier was not allowed to make any profit above a prescribed level, it had reduced incentives to engage in transactions if it was near the profit constraint. Instead, the regulatory system gave carriers an incentive to maximize telephone *traffic*, because this would lead to an increased physical plant which translated into a larger rate-base and consequently higher profits in absolute terms. It also led to a larger organization.

In such a system, telephone carriers had no particular incentive to offer certain specialized privacy services. If, on the other hand, regulation controls prices rather than profits, these incentives may well be changed in favor of offering privacy technology. For instance, carriers had less incentive to offer call-blocking devices and services such as "Caller I.D." because it might reduce the level of total traffic. The very nature of Caller I.D. is that it gives customers the ability to "refuse" to accept selected traffic if desired.

A second reason for governmental reduction of privacy-generating transactions is the clash of conflicting policy objectives. Consider the U.S. government's efforts to establish the "clipper chip" standard as a *de jure* encryption system for America. The clipper chip involves an encryption algorithm embedded in a microchip. This algorithm is crackable by design, through the simultaneous use of two separate electronic "keys" to be maintained by two agencies of the federal government. These keys are supposedly to be available only through a court order to both that authorizes wiretapping. The purpose of this system is to permit governmental eavesdropping for court-authorized law-enforcement and national security purposes, while reducing the possibility of abuse. It

also means that non-crackable encryption may be unavailable in the market.

Examples for the Market and Regulatory Approaches

The working (as well as non-working) of the market mechanism in responding to privacy concerns can be demonstrated through several current communication issues.

Telemarketing

Because privacy and access are of value to parties in a telemarketing transaction, exchange transactions will emerge once they become technically feasible. How could this happen? Telecommunications equipment and service providers will offer the capability to select among incoming calls electronically. Once choice is available, callers will have to offer incentives to have their unsolicited calls accepted. What will emerge is a system of access charges.

Such a system might be described as *Personal-900 Service*, analogous to 900-service in which the caller pays a fee to the called party. This service could, for example, block incoming telephone calls to a consumer with an electronic message and a series of options. The caller would be told that the customer charges commercial telemarketers (but not others) for his time and attention.

Individual customers could set price schedules for themselves based on their privacy value, time constraints, and even the time of day. They would establish a "personal access charge" account with their telephone company, or enhanced services provider or a credit card company. By proceeding, the telemarketer enters into a contractual agreement. The consumer could override the charge by entering another code. The billing service provider would then automatically credit and debit the accounts in question.

Such a system could negatively impact the business of telemarketers. Currently, they "externalize" some of their costs by accessing customers at home at no charge other than the communication charge. Right now, consumers do not yet have the means to make the telemarketer compensate them for their attention. (In broadcast TV, the audience gets at least to view an entertainment, sports, or news program.) Under personal-900, telemarketers will be forced to pay more for consumer access.

Consumers will benefit from the payment they receive for accepting calls. Some might even become "professional call-receivers," though telemarketers will no doubt refine ways to identify the most likely buyers. Telemarketers will become more selective in whom they try to reach, and spend more money on "fine tuning" their customer lists. They may keep track of who does not buy, and they may exchange such lists with others. (This leads to a new potential privacy problem.)

Markets in access will develop. Consumers will adjust the payment they demand in response to the number of telemarketer calls competing for their limited attention time. If a consumer charges more than telemarketers are willing to pay, he can either lower access or will not be called anymore.

Yet, consumers, too, will bear some of the portion of these costs; first, by way of higher prices for telemarketed products. The extent to which these costs can be shifted by telemarketers to buyers depends on the relative elasticities of demand and supply. Where telemarketers are in strong competition with other forms of marketing, and where consumers are price-inelastic, telemarketers will bear most of the added cost.[8] Consumers will also bear a portion of the costs in the form of higher telephone rates to cover the reduced traffic due to access charges. Telemarketers will similarly bear some of that cost through high telephone charges.

Wireless Transmission

Market forces may also be able to resolve the unauthorized eavesdropping of wireless communication systems such as cellular and cordless telephones. True, such monitoring is illegal for cellular calls (though not for cordless phones), but it is widely practiced by scanning hobbyists as well as investigators).

As discussed earlier, eavesdropping is inefficient because it forces the participants in a communication to disguise the content of their transmissions. Thus, there are incentives for cellular service providers or equipment firms to offer scrambling devices.[9]

Encryption systems require extra equipment and may increase the amount of spectrum required for a given quality and information content of a signal. Customers who value privacy sufficiently will be willing to pay for the increased resource cost.

A special problem of privacy in mobile communications is that the person initiating the call to a mobile customer does not pick its privacy level, and may be entirely unaware of any jeopardy. This "negative externality" suggests that a regulatory disclosure

requirement is necessary, such as some form of a signal which alerts such a caller to the presence of radio-segments in the transmission path.

Data Banks

Companies often sell or pass along information about their customers to others, for a variety of purposes. Insurance companies want to know the accident and medical history of new applicants; stores, whether new customers are credit-worthy; employers, whether job applicants have criminal histories; doctors, whether a patient has brought a malpractice suit in the past.[10]

In America, individuals, firms, and governments have, within some restrictions,[11] a substantial right to collect and redistribute personal and financial data about individuals. One could conceive of a market transaction system by which consumers offer companies payments to delete such information or refrain from distributing it. But could such a system work? In any transaction, both parties remain with information about it. The problem is not usually that a party saves that information, but rather that it disseminates it to others. The regulatory approach restricts some of these transfers. Could a market work instead?

The answer to this question is usually no. The reason for this can be found in the logic of reselling information. In many cases, the holder of information about a second party could share that information with a third party at a higher price than the resulting reduction in value to him. Take, for example, a piece of credit history information on individual A that is worth $5 to B, as long as B retains the information exclusively. If B distributes the data to another party, C, the direct value of the data to B may drop a bit to, say, $4, or stay at $5. (It is one of the peculiar economic properties of information that it can usually be shared without any or only little loss of usefulness to its holder. Exceptions are business and trade secrets.) Suppose C, too, is willing to pay up to $4 for the same information, because it is of similar usefulness to him. Then, the total value to B of not destroying the information is $8. And why stop at two beneficiaries? B could resell the information to D, E, etc. In each case, the reduction in value of the information to one of its holders may be less than what another party will gain by obtaining it.[12]

Hence, the information will spread. Accordingly, the subject of the information, individual A, might have to expend a significant amount of money to repurchase the information. If it is of use to 100 firms, each valuing it at $4, it would take a $396 "bribe" for A to keep B from reselling it.

At the same time, any effort by A to pay a high price to B for non-revelation will likely raise the value of the information to B, C, etc. What is A trying to hide? Thus, the more important the information is to more parties, the less affordable is a market transaction to purchase privacy. Even if A could pay B to withhold the information, it may not be possible in practical terms. One of the characteristics of information is that its exclusivity is almost impossible to acquire once multiple parties have access to it. Only where information is of little use to others are privacy transactions likely.

An example is a video store. Such a business could advertise that its policy is to guarantee privacy. It would gain customers, and since information about movie preferences is not usually very important to many other parties, it would lose little. (The interest in political figures and celebrities is an exception.) In contrast, it is hard to imagine a credit card company willing to be compensated for non-disclosure to other credit-extending firms. The value of preventing credit-fraud is so great to so many firms that any payment to undermine the reporting system would have to be quite high. Yet, video-store disclosure is prohibited by law, while credit-reporting is legal. The reason is probably that the loss of information-value was low for video-viewing and no economic interest therefore mounted a fight against such legislation.

Consumers could attempt to stop personal data from being released to a third party be preferring to do business with firms that agree to destroy such data. But companies would charge customers higher prices to compensate for the lost information resale. Furthermore, once many companies start refusing to sell information, they will have less information and hence greater risk, which would be reflected in the price of products.

In any event, any negotiating approach will work only for transactions between individuals and businesses. If the information is obtained by government, fewer market-based incentives exist to prevent transfer of the data. This is one reason why government agencies are becoming so aggressive in selling information to others. They have little business to lose. Where else could one go to get a driver's license?

Additionally, data bank activities include several negative externalities, such as incorrect information contained in data banks.[13] For the database providers, such inaccuracies, while bothersome and somewhat

reducing the database value, may not justify the cost of attaining great accuracy. Yet, for the data subject, the cost of an inaccuracy can be very high.

Currently, there is a right to collect, distribute, and utilize personal data. What then if the rights were reversed and one would have to get a person's permission before retaining, transferring, or utilizing personal data about him?[14] If the information is of value to a bank and other credit institutions, they would acquire it by compensating the customer. Given the collective value of the information, such a transaction would be likely. Hence, the information would be circulating. Consumers would be a little richer than before, but the information would still be in the public domain.[15]

In conclusion, for personal data banks that contain information about individuals, market transactions are either unlikely where the information is of use to many others, or it will be acquired by them, even at added cost. In either case, the personal information, if valuable, becomes "public" information.

Intra-Organizational Communications

The proliferating intra-organizational private networks create privacy problems of another kind. They enable employers to track employee calls and their physical presence, location, and productivity. They can eavesdrop on conversations, read e-mail, and copy facsimiles.

Some firms, including airlines, mail-order houses, and telecommunications companies, monitor their workers electronically to assess their speed, accuracy, courtesy, and compliance with legal requirements in dealing with customers over the telephone. Labor unions have been pressing for legislation that prohibits such activity, requires employers to notify workers when monitoring occurs, and protects the privacy of data obtained in the monitoring process.[16]

In theory, employees would normally prefer to work for employers who do not eavesdrop on them. The exception might be if employees believe that a restrictive environment enhances productivity, and that they share in its rewards.[17] In practice, mobility and choice are limited for most employees. Because of the associated high transaction costs, the market will probably not succeed in solving privacy problems in most intra-organizational networks.

Thus, markets in privacy protection are more likely to work for telemarketing and mobile eavesdropping. They are less likely to work for data banks and corporate networks.

Selling the Right to Privacy

So far, we have analyzed the role of markets in the provision of privacy in a largely pragmatic way: will it work? But, at least as important is the normative question: *should* privacy be part of a market? While the market approach could be efficient on economic grounds and would differentiate according to needs, efficiency is not the only value to be concerned about. Just as there are economic tradeoffs, so are there non-economic ones.

First, it should be clarified what types of rights are being considered. We are *not* talking about political rights that protect the spheres of the individual versus encroachments by the state. The individual's right to be free of unjust searches or unlawful wiretaps is not a matter for market forces, for fundamental reasons as well as practical ones. (That the reality of protection often requires private legal resources is another matter.)

Such political rights and their application across society are fundamental to democratic societies. The commercialization of political rights is a weakening of the democratic system. But negotiations of private parties among themselves about the way they transact with one another are in another class. Claims against private parties are different from claims against the state.

There are a number of arguments against treating rights as a commodity. They were classified by economist Arthur Okun, when serving in Washington as Chairman of the Council of Economic Advisors, as libertarian, humanistic, and pluralistic.[18]

To libertarians, a distribution of privacy rights on a free-market basis would provide no protection for citizens against encroachment by the state. The only effective limits on government are those established through constitutional means. Therefore, any system which allocates privacy according to the open market would also need constitutional provisions that bar infringements by the state.

A second view is the humanistic one. Rather than distribute resources according to an individual's ability to pay, a humanistic approach allocates resources differently. For the philosopher John Rawls, the principle for such allocation would be according to the values individuals would give resources if the persons were placed in a societal "original position," without any knowledge of their future self-interests and needs. Rawls believes that people would distribute basic liberties equally out of "mutual respect" for their fellow

human beings. Even if one accepts this view, which implies risk-averse individuals, it is relevant to the initial distribution of rights, rather than to the question of how people would use them subsequently.

A related view is the instrumental one. Privacy is a factor in public welfare and safety. Privacy permits other activities to occur which are essential for society's functioning, for the exercise of other rights, and for many economic activities.[19]

Perhaps the most prevalent argument is a pluralistic one. This view does not accept the belief that efficient allocation is the paramount societal goal. Thus, some resources, such as privacy allocations, would be designated as inalienable rights that are protected from encroachment by the open market system.

This position leads to several responses to the notion of transaction-generated privacy:

(1) Privacy is a basic human right, and is not subject to exchange transactions.
(2) A transaction system in privacy will disproportionately burden the poor.

To state that privacy is a basic human right is a noble sentiment, and one with which this author is in accord: but it does not follow that privacy, therefore, is outside the mechanism of transactions among individuals. A right may be acquired without a charge and be universally distributed regardless of wealth, but it is in the nature of humans to have varying preferences and needs, and to exchange what they have for what they want. Whether we like it or not, people continuously trade in rights. In doing so, they exercise a fundamental right—the right of free choice.

In most cases, a person does not so much transfer his or her right to another but chooses not to exercise it, in return for some other benefit. A man has the freedom of his religion, but may reconsider for his spouse's sake, or vice versa. One can be paid to assemble or not to assemble, to forgo bearing arms, travel, petition, or speak. Students have the right to read faculty letters of recommendation written in their behalf, but they usually waive that right in return for letters they hope will have greater credibility. Votes are not formally for sale, but candidates and parties vie with each other in making promises to benefit voters and interest groups, and if they renege on their part of the bargain, they may be punished at the next election.

These departures from textbook civics are socially undesirable if the rights in question were given up under some form of duress, for example if in a single-employer town the workers must agree, as a condition of employment, not to assemble. But when an informed, lucid, and solvent citizen makes a choice freely, the objections are much harder to make. They then boil down to a transaction being against public policy, often because it affects others outside the parties to it (i.e., "negative externalities"). To make such transactions illegal, however, does not stop many of them, given willing buyers and sellers, but it makes them more difficult and hence costly. The extent of the success of such a ban depends, among other factors, on the ability of the state to insert itself into the transaction. In the case of privacy, which by its nature is an interactive use of information, such insertion is difficult. If it becomes illegal to offer compensation to obtain consent, one can expect imaginative schemes to run circles around such a prohibition. Indeed, the success of government enforcement would depend on privacy-intrusive actions by the state into private transactions. As important as the right to privacy is, it will not necessarily override other rights, such as the right of free choice, the right to know, and the right to be left alone by government. A balancing will occur.

The second objection to transactions in privacy is that they disproportionately harm the poor. Those suffering from financial pressures and ignorance will sell their privacy rights to rich individuals and institutions. In many cases, a poor person's priorities may not include privacy protection. In others, however, the opposite may be true, and poor people need privacy more than those who can afford to create protective walls and screens for themselves. Yet, the same poverty condition may also make a poor person a less attractive target for commercial intrusion by those marketers who prefer to make a pitch to higher-income individuals.[20] Thus, it is quite possible that the poor, if identifiable, will have fewer paying offers to accept a telemarketing call than will the middle class.

Business users of personal information also object to transactions. They are worried that while today they have relatively free phone access to individuals, or to data about them, a system where they might have to pay compensation in return for consent might become too expensive. They are correct (although some of the cost will be shifted to consumers, as discussed), but what can they do about it? A telemarketer's access to an individual, even if sanc-

tioned by law, requires the latter's cooperation. Right now, individuals do not yet have the means to make the telemarketer compensate them. But, no doubt, this will change in the near future when equipment makers and service providers will enable consumers to charge for access. When this happens, those who live by the free market will also have to play by its rules.

A Differentiated Approach

This article has pointed out that, in many cases, market transactions can generate privacy protection. But it has also described cases in which markets fail or transactions are precluded; and it has identified troubling questions and objections to the notion of markets in privacy. This analysis leads to a conclusion that privacy, being a broad umbrella for a variety of issues, cannot be dealt with in a single fashion. A differentiation of approaches and a multi-level perspective on privacy are necessary.

Privacy Market Failure

A first set of protection issues are those where transactions are not forthcoming, indicating a structural market failure. Examples include inadequate protection of taxpayer information by government; or where transaction costs are high. In such cases, the policy preference of the community should be translated into government policy, either by legislative rules or, where important considerations exist on the other side, by letting it continue.

Unfavorable Privacy Market Outcomes

A second set of issues exist where market transactions take place, but we do not like the outcome due to a variety of other societal goals; for example, data banks that contain personal information that is available to other buyers. Since, for society, economic efficiency is not the only value, it can institute regulatory restrictions. But it must be recognized that, given the initial logic of the exchange transactions, they will find a way to assert themselves in other ways, thus undercutting the effects of the restrictions and leaving them more in the nature of a societal statement of intent.

Privacy Market Constraints

A third set of privacy problems occurs where transactions would be possible but are constrained by either market structure, governmental restrictions, or the original allocation of rights. Individuals may be ignorant of the use to which transaction information is being put, and may require disclosure of such use to make them informed market participants. If society is serious about protecting privacy, it would assure that legislation, regulation, and court decisions would make these transactions possible. Similarly, for markets in information to exist, it may be necessary to allocate initial property rights in them. We discussed earlier the allocation of rights of access control in telemarketing as an example.

Market Privacy

The final set of is those where the level of privacy protection can be set by free exchanges by individuals. An example is when telecommunications users seek encryption devices to protect wireless transmissions from reception by third parties. There is no reason for state intervention in such situations.

Obviously, some issues will span more than one category. A regulatory protection might be unnecessary for most people on a particular issue, but some categories of people might have specialized and different needs. Given this framework, a tiering structure for privacy protection could be designed. Certain levels of privacy not developed by markets would be provided through legislation and through constitutional interpretation. Remaining elements of privacy would be left to the market to allocate.

The multi-faceted approach to privacy protection presented in this article may appear complicated. Granted, a policy of prohibiting practices which violate privacy has the attractiveness of apparent simplicity. In contrast, the multiple tiered approach presented in this article allows for each privacy issue to be resolved in a variety of ways.

Additionally, a competitive telecommunications environment can support privacy. Some have argued that one advantage to a monopoly in telecommunications is that it can better protect the privacy of its customers. This article, however, has given examples of how monopoly carriers can have incentives that would be adverse to an offering of privacy services, and how competitive telecommunications can develop solutions to consumer and business demands for privacy. Thus, competitive and diverse telecommunications can be a help to privacy protection and not a threat to it.

The dilemma of privacy protection has existed since the beginning of telecommunications and will continue. There is no single privacy "solution" or measurable equilibrium point, which implies that any

protection system will need to be able to reflect current technical, social, political, and moral contingencies. The use of a privacy advisory board and privacy principles can provide approaches to privacy issues in many cases, and to the question of how to allocate rights initially.

The centralized European system is not a suitable model. The United States needs to conceive a privacy strategy appropriate to its greater reliance on market forces.

The creation of a Privacy Advisory Board would provide a semi-official body that can advise, study, educate, anticipate, identify gaps, and serve as a catalyst. It would help to develop policies that balance various societal interests and to steer a course between anti-technology luddism on the one hand and a technocratic disregard for privacy interests on the other. Technology outpaces regulatory treatment. Legislators and regulators have often either let themselves be steamrollered, or else they have retarded innovation while learning about an issue. Both choices are unacceptable. In privacy, too, there is a learning curve. Policy wisdom comes to those who are prepared. ntq

For a complete bibliography, please contact Technology Futures, Inc. at (800) 835-3887 or (512) 258-8898. This article was reprinted with permission of the Office of Communications, United Church of Christ, 200 Prospect Avenue, Cleveland, Ohio 44115-1100; (216) 736-2222. Reprints are available for $5.00 per copy.—Ed.

---

[1] R. Coase, "The Problem of Social Cost," *The Journal of Law and Economics*, Vol. 3 (October 1960):1-44.
[2] Ibid., p. 96.
[3] Posner, *The Economics of Justice*, p. 255. *Pavesich v. New England Life Insurance Co.*, 50 S.E. 68 (1905) (the unauthorized use of a gentleman's photo in an insurance advertisement).
[4] Quite possibly, such policy would shift rights and thus wealth to large organizations, such as data holders or communications carriers.
[5] This is more likely to cover primary providers of major services than more specialized privacy problems.
[6] This would be the case where the cost to telemarketers to initiate calls, including in terms of reputation, would be low relative nuisance value to the consumer. The telemarketer's strategy would not be openly harassing, since that would be illegal, but the income from non-calls would be part of its overall revenue stream, hence part of its incentive structure.
[7] Copyright protects only the form of presenting the information, but not the information itself.
[8] One might argue that telemarketers will attempt to avoid absorbing this added cost by increasing their prices and then advertising a "fictitious" discount in return for a customer giving access rights. But such a practice will not succeed in a competitive environment where the initial price increases cannot be sustained.
[9] For example, GTE released in 1991 an encryption system for the cellular-consumer market. GTE Mobilnet developed the system because some customers—mostly government accounts and defense contractors—were concerned about the use of scanners that can monitor radio waves over which mobile-telephone signals move.
[10] The consumer information business is a multi-billion dollar a year business, centered around credit bureaus such as Equifax, TRW, and Trans Union. It has been estimated that the average American is on 100 mailing lists and 50 databases. S. E. Fisher, "What Do Computers Know About You: Personal Information Too Readily Available," *PC Week*, Vol. 8, No. 6 (February 11, 1991):156.
[11] E.g., the Fair Credit Reporting Act and many state statutes.
[12] The analysis takes factors such as timeliness, authenticity, and integrity as given.
[13] J. Rothfeder, *Privacy for Sale, How Computerization Has Made Everyone's Private Life an Open Street* (New York: Simon & Schuster, 1992).
[14] Consumers will increasingly demand compensation for giving out commercially useful information (Westin, *Privacy in Western Society*).
[15] One obstacle is that consumers will have to police companies to make certain that they do not utilize information without first making compensation. This difficulty could be dealt with through the assistance of a service provider who would run "key word" searches to determine if a person's name and personal data are utilized for any uncompensated purpose. This, however, would also raise a new type of privacy concern.
[16] 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.
[17] A. A. Alchain and H. Demsetz, "Production, Information Costs, and Economic Organization," in R. A. Posner and K. Scott, eds., *Economics of Corporate Law on Securities Regulation* (Dubuque, IA: Brown, 1980), pp. 12-19. Surveys indicate that most employees do not oppose any and all monitoring, only those without cause, conducted unfairly and without proper procedures, and without employees' due process rights.
[18] A. Okun, *Equality and Efficiency, The Big Tradeoff* (Washington, DC: Brookings Institute, 1975).
[19] M. Rotenberg, "Communications Privacy: Implications for Network Design," *Communications of the ACM*, Vol. 376, No. 8 (August 1993).
[20] Telemarketing fraud, on the other hand, may be targeted to the least educated and most desperate in society.