Telecom Privacy Policy Elements

The development of telecommunications services has accelerated in recent years. But technology can be a double-edged sword. New services raise new problems, or old ones in new guises. One of these is personal and business privacy. Privacy as a problem has recently surfaced in the context of automatic number identification (ANI) services. But the issue is really far broader, and ANI is merely a manifestation of the more generic issues inherent in protecting information in an increasingly open network system.

This is not to suggest that privacy protection in telecommunications is a new issue. In the past, manual operators,[1] party lines,[2] and the absence of a warrant requirement for wiretapping[3] all created their own problems. The first patent for a voice scrambling device was issued in 1881, only five years after the invention of the telephone. But those problems were overcome, and relatively strong expectation of privacy developed in time. Today, a new generation of privacy problems has emerged (see *Telecom Services Raising Privacy Concerns* on p 15). The reasons include:

(a) more and more transactions are conducted electronically;[4]

(b) it has become easier and cheaper to collect, store, access, match and redistribute information about transactions and individuals;[5]

(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.

Concern with electronic privacy has led to different policy approaches. West-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.[6] 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 Federal Communications Commission (FCC), and they often addressed only a specific issue of concern to a legislator who initiated the action.[7]

Even without seeking omnibus legislation, approaching telecommunications privacy policy in a broader fashion may permit the commission to look at the issues in a forward-looking way that balances the various societal interests. Privacy problems recur in various guises, and it is helpful to examine them systematically and develop more general regulatory principles. This would have several advantages:

1 Offerers of new services would know in advance how to structure their offering and have them approved (where required) in a speedy fashion.[8] Even where Public Service Commission (PSC) approval is not necessary, such principles may raise the sensitivity of service providers to privacy concerns.

2 A broad set of principles would help in structuring consistent policies that balance various societal interests and 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; regulators have often either let themselves be steamrolled, or have retarded innovation while learning about an issue. Both choices are unpalatable. Policy wisdom meets the prepared.

3 A broader approach would help to define expectations about privacy. And

Noam Proposes Telecom Privacy Principles

Individuals and organizations in the United States and other countries are invited to submit comments on a proposal to establish principles of privacy in telecommunications services, in response to a request issued by the Public Service Commission of the State of New York on January 31, 1990.

Eli M Noam, a commissioner, proposed the enquiry and submitted a background paper describing the need for a telecommunications privacy policy, countervailing interests, and existing federal statutes. A number of general principles of privacy protection are proposed.

In addition to his responsibilities on the PSC, Noam is a professor at Columbia University, and author and lecturer on telecommunications policy issues. He is also a member of the *TDR* Advisory Board.■

Comments should be addressed to: The Secretary to the Public Service Commission, Three Empire State Plaza, Albany, NY 12223, USA.

Noam

expectations have concrete implications. In numerous cases,[9] the US Supreme Court has consistently ruled that privacy protection is governed by the standard of reasonable expectations. For example, if one reasonably does not expect monitoring, such monitoring would be an invasion.

4 If privacy protection proceeds in an *ad hoc* fashion, it may well be expensive to superimpose protection on existing hardware and software systems. It is likely that it is much cheaper for manufacturers to configure software programs in advance if they are aware of privacy expectations.

Privacy in the telecommunications sector, broadly defined, consists of two distinguishable but related aspects:[10]

(a) the protection against intrusion by unwanted information, sometimes termed the 'right to be left alone',[11] and which is an analogue to the constitutional protection to be secure in one's home against intrustion 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.[12] A related aspect is the security of information about oneself from tampering by others.

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:

1 *Only the guilty need privacy*

To the contrary, privacy is one of the touchstones of a civilized and free society.[13] 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.[14]

2 *Privacy is a drag on the economy*

There are also good economic arguments for 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. Information often has actual value, and since much of it has no protection through property rights, it must be protected through confidentiality or secrecy.[15] To permit its easy breach[16] would lead to a lesser production of such information.

Similarly, anonymity may increase economic risk-taking; certain investments may be curtailed if the identity of their investors is 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. 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.

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.

3 *Privacy is of interest to a small elite only*

On the contrary, attention to privacy is widely shared. For example, according to information from the New York Telephone Company, 34% of all residential households in Manhattan and 24% of all its residential households in the state have unpublished telephone numbers at subscribers' requests. 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.

Another indication is provided by a survey conducted by the American Express Company among its card holders. Ninety percent felt that mailing list practices were inadequately disclosed, 80% thought 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.[17]

A 1988 survey by the Massachusetts Executive Office of Consumer Affairs of the main consumer complaints found them topped by telemarketing and promotional mailings.[18]

Pacific Bell planned in 1986 to sell subscribers information such as new phone numbers. More than 75,000 complaints came in, and the company backed off.[19]

There are also practical reasons for being forward-looking on this subject. The European privacy requirements mentioned earlier (and their coordination through a recently ratified European Convention) may affect the United States. These requirements threaten to restrict data flows to countries whose privacy protection is less assured – including the United States. And this, in turn, may jeopardize the role of New York as a global center for data-intensive transactions. Similarly, it may limit its role in remote-access data processing and in online database publishing. Arguably, the policy consequence should not be to establish strict rules matching the Europeans' often heavy-handed approach, but instead to structure a more flexible system: a framework in which the user would have several 'privacy options' of service, which would thus provide a choice in the level of information protection. Thus, a

transnational user could flexibly match the transborder privacy requirements of other countries by selecting the appropriate domestic privacy protection level.

Will competition take care of privacy problems? Not necessarily. A competitive environment may resolve some privacy issues, especially if it is possible for a user to select a service provider which offers the desired level of privacy protection. Carriers would lose business if customers felt unsure about privacy of usage. But in many other instances the greater openness of a competitive system and the greater complexities of its multiple networks may also mean a greater openness of information.

It is probably easier to restrict the dissemination of information in a monopoly setting. By its nature a network is a sharing arrangement. In the past this sharing encompassed mostly physical assets such as trunks and switches. But as the 'intelligence' of networks increases, and as enhanced service networks and physical networks evolve that participate in communications services, the sharing reaches also data and other informational resources.

Hence, a major question that needs to be addressed by the commission is the overall impact of a more competitive environment on privacy protection.