

Chapter 28

Telecom Regulation in the Information Age

Rohan Samarajiva¹

1.0 Introduction

Advanced telecom networks, also known as public information infrastructures, are to be built in the United States and in most other countries by private sector companies and not as public-works projects (Canadian Information Highway Advisory Council 1995; US Secretary of Commerce 1994). What this means is that the enormous investments that are being, or will be, made in public telecom networks must be recovered with a return considered adequate by the investors. The big question, therefore, is not what can or cannot be done with the technologies, existing and to be designed, but which technological configurations will allow investors to recover their investment. Unless significant numbers of people use the services provided over the upgraded public networks, it is unlikely that investors will earn returns. Regulators must take an interest in conditions that affect usage for a number of reasons.

- In situations where network upgrading projects are funded in part through cross-subsidy by customers of monopolistic or oligopolistic firms subject to regulation, or benefiting from exclusive franchises, or where financial distress of holding companies can affect regulated activities, regulators must take an interest.
- Standard economic wisdom posits that customers subject to unacceptable commercial practices will respond by withholding their business. However, it is also well known that exit options are not unconstrained in the real world, especially in essential telecom services. Where exit is constrained, voice becomes the alternative (Hirschman 1970). Customers are likely to direct their voice at regulators more than at the offending firms. Regulators have to be prepared for, and try to pre-empt customer complaints or get ambushed by them later.
- Changes in regulated industries, including the easing of entry barriers, the phasing out of rate of return regulation, the rising importance of interconnection (and associated information-transfer issues), rapid technological change, and changes in customer expectations – particularly with regard to more control over services – all create new problems for regulators. As routines are disrupted by new ways of doing business, customers as well as suppliers of regulated services face uncertainty, which can very easily lead to mistrust and even anger. As with voice, anger can be directed at regulators as well as at the regulated firms.
- The above mentioned changes in regulated industries give rise to a host of new inter-firm relations and attendant problems. Resolving inter-firm conflicts can

easily lead to harm to customers. For example, regulators' efforts to "level the playing field" for providers of long-distance and enhanced telecom services in the US has, in some instances, led to indiscriminate release of customer records (Burns, Samarajiva & Mukherjee 1992).

There has been much discussion of new "killer applications" that will ensure significant usage of the upgraded public telecom networks, and thereby their economic viability. At this stage, it is only possible to state that the hypothesis of video on demand being the "killer app" has fallen out of favour (Hough 1995). Instead of speculating on an alternative "killer app," it may be more realistic to approach the problem of usage of upgraded public networks by recognising that they are virtual public spaces and analysing the principal activities that take place in public spaces (Samarajiva 1994). The prototypical public space was the Roman Forum. Every civilisation had its own form of proximate public space, but the Roman Forum is discussed because it is among the best known (e.g., Romanelli 1929).

The Forum had specific architectural features and changed over time. It served four principal functions.

1. Being a location where large numbers of people congregated, the Forum was a natural place to meet others and initiate face-to-face communication. It had a *meeting-place function*. This included pre-planned meetings between earlier acquainted persons and serendipitous meetings between hitherto unacquainted persons. Though initiated in public, the actual interactions could be private.
2. From the beginning, the Forum was a place to buy and sell. It had a *market function*. Markets occupied parts of the Forum, generally separate, but proximate to the politically and symbolically important sites. Vendors were attracted to the Forum because of access to large numbers of potential buyers or audiences. Buyers included those who came specifically for that purpose and those who came for other reasons but were attracted by the presence of the vendors.
3. The Forum was a site for political discourse. This best known function may be described as the *expression function*. Orators spoke at the Forum because it concentrated audiences. Those who wished to obtain political information went there because it was known as a site of political discourse. The political functions were concentrated in a part of the Forum known as the Comitium. Access to political power afforded by this space was contested.
4. Over time, the Forum became a location for religious and state symbols and monuments. This may be described as a legitimising function. The state, which built and maintained the Forum, exploited the concentrated attention of the multitude coming to the Forum through this symbolic activity.

Key issues affecting usage of advanced telecom networks may fruitfully be examined in terms of the first three of the above functions. For the sake of brevity, the discussion excludes the fourth function and is illustrated with US examples only.

2.0 Meeting-place Issues

The “old” telephone networks primarily served the meeting-place function. Public telecom and computer networks of the mid 1990s constitute, among other things, virtual meeting places. These networks enable a person to initiate dyadic or small group communication with others among millions of connected persons, and one or more among these millions to initiate communication with that person. The “publicness” of a space depends on openness to initiation of communication among inhabitants rather than the terms and conditions of access to that space. The existence of usage fees for accessing a network does not, therefore, vitiate the publicness of a virtual space. The moment of “entering” virtual space by lifting the telephone handset or logging on to a computer network is similar to entering a proximate public space. Contact may be initiated with a person or persons in that space at that moment, for example, a chat-line or the “talk” mode in the Internet; or later when the person or persons log on; or by initiating contact with those in physical private and public environments abutting the virtual public space, such as a telephone user at home or in a pub with a telephone.

The proposition that public telecom and electronic mail networks are virtual public spaces may be challenged by the apparent lack of temporal co-presence between inhabitants of virtual public space. It may be difficult to accept that the millions of potential called parties are co-present on the network at any given moment. They may be out boating, at lunch, or dead. The frequency of “telephone tag” may be used to question the claim of co-presence. Nevertheless, the claim is defensible insofar as social space is constituted when one party believes the other is potentially co-present. Discovery of the other’s absence terminates a private space. In a public space, the expectation is not one of certain communication with a particular person, but of potential communication with some person. The absence of a particular individual does not negate the public space.

Generally, actors do not establish interpersonal contact with totally unknown persons in virtual or proximate public space. It is more common for persons to navigate public space to establish contact with a known person or persons, at which point the dyad or larger group effects a complete or partial withdrawal from the public space into a private space. In both kinds of public space, the possibilities of unintentional collision exist in the forms of physically bumping into bystanders and dialling wrong numbers.

2.1 *Privacy*

A definition of privacy may be developed from research on face-to-face human interactions in public spaces. Human interactions in “proximate” public spaces such as sidewalks are governed by mutually accepted ground rules rather than formal rights. Goffman has studied these ground rules in detail. He saw ground rules regulating dealings between those who share hardly any common organisational or family affiliations, the classic examples being people navigating busy streets, signalling directional changes and rights of way to total strangers. Goffman (1971, p. 198) identified one important ground rule as:

[...] in Western society, as probably in all others, there is the ‘right and duty of partial display.’ Two or more individuals present together have the right and duty to make some information generally available concerning their relationship and the right and duty to leave unsigned other information about their relationship.

Drawing on Goffman's work and subsequent scholarship (Altman 1975; Petronio 1991; Ruggles 1993), privacy may be defined as the capability to implicitly or explicitly negotiate boundary conditions of social relations. The definition includes control of the outflow of information that may be of strategic or aesthetic value to the person and the control of the inflow of information, including initiation of contact. This definition does not posit privacy as a state of solitude, as suggested by definitions such as "the right to be let alone".

Privacy violations would lead to the avoidance of the network as a meeting place (if alternatives exist) or the use of various defensive measures driven by mistrust (if there are no alternatives). Trusting interaction in a public place requires that individuals can control release of their access information and that certain forms of eavesdropping, in relation to content of conversations and the interaction, can be avoided. Access information has been defined as "information disclosed in public that can be used to locate an individual at some future time." In addition to a person's home address or place of work, knowledge of one's full name, phone number, neighbourhood, habitual routes, and hangouts can serve as access information. A certain degree of random eavesdropping is acceptable in public spaces. However, eavesdropping in the form of systematic surveillance is not. All forms of eavesdropping are unacceptable for interaction in private spaces. The ongoing redesign of public telecom networks to systematically track communicative interactions and, in some cases, make it possible for government agencies to eavesdrop on private conversations, poses a serious threat to the meeting-place function of telecom networks.

One manifestation of the redesign that has drawn public attention is Calling Line Identification (CLID), known also as "Caller ID." CLID delivers to the call-receiving party information (in computer-processable form) that a call was made from a specific telephone at a specific time. This type of information that is a by-product of an interaction is described as transaction-generated information (TGI). In conjunction with contextual factors, telephone TGI may yield a significant amount of additional information. For example, if the called number is that of a used-car dealership, it may be inferred that the person assigned the captured telephone number (or a member of that household) is in the market for a used car at that time. In addition the captured information includes access information.

Reduced control over outgoing information enables more parties (including individuals and organisations having no direct dealings with the user) to learn more about the user (particularly by using the telephone number and other identifiers to access personal information in other databases) and to locate and contact the customer by phone, mail, or in person. Thus, the loss of control over outgoing information leads to a loss of control over incoming information and face-to-face interactions as well. The user need not subscribe to CLID to suffer these negative consequences. The majority of subscribers and users of telecom monopolies who choose not to subscribe to this discretionary service will still undergo a reduction of ability to safeguard their privacy. Lacking a practical alternative, they will continue to use the network, but will be mistrustful and angst-ridden.

Surveys (e.g., Katz, 1991) indicate the existence of significant public concern about wiretapping in the US. In addition, the current confused state of law regarding eavesdropping on non-wireline conversations in the United States (cordless/PCS appears

to be unprotected, while cellular/PCN may be protected in law, but not in practice), is likely to aggravate public concern over time. In addition, the national security concerns that legitimised US encryption policy for many decades have lost legitimacy in the post-cold war era. Contemporary encryption debates in the US have crystallised around “key escrow” legislative proposals, whereby cryptographic systems will have legally mandated “back doors” that can be accessed without the knowledge of the users under certain specified conditions. The extent and nature of technical and legal wire-tapping capabilities on the one hand and the consumer use of encryption on the other affect privacy in relation to content of communication. Even if content surveillance is minimised or avoided, surveillance based on TGI will still be possible. Indeed, greater freedom for law enforcement agencies to access telephone and credit-card TGI is a central element of the Clinton Administration’s continuing legislative efforts on anti-terrorism.

2.2 Addressability

The network’s meeting-place function rests on addressability. In order to interact with a person in proximate space, awareness of co-presence is a minimum condition. The ability to initiate an interaction with one person requires some form of “address” in the form of a name, or even eye-contact, singling out, and communication of the wish to initiate contact, in the absence of a name. These minimum conditions must be met in virtual space too. One of the greatest assets of the conventional telephone network is its addressing system in the form of different sequences of numbers, originally reflecting spatial location but increasingly disconnected from it. Technological and economic change are increasingly threatening the established practices pertaining to addressing, making it necessary for regulators to pay attention to this hitherto “taken-for-granted” aspect of the network.

Primarily due to profligate use, such as the allocation of generally under-utilised blocks of numbers to suppliers of services such as paging and cellular services, but also due to growth of access points to public telecom networks, shortages of telephone numbers have begun to appear. What was once considered to be an inexhaustible resource has been discovered to be limited. The problems are being exacerbated by the transitions from calling locations to calling persons, and from monopoly to competition in local-exchange services.

Prior to the emergence of mobile telephony as a significant phenomenon, public telecom networks were utilised to connect to telephone instruments fixed to locations associated with called parties. The new mobile telephony, particularly in the ideal form of a shirt-pocket or wrist telephone, enables a called party to be reached directly, irrespective of location. The transition period between these two forms requires more numbers than either the pure location-based paradigm or the pure person-based paradigm. Individuals continue have separately numbered telephones for locations associated with them (e.g., home, office, car, boat). Transitional person-calling systems such as “follow-me” services merely overlay a “personal” telephone number atop the location-specific numbers. The result is an even greater usage of telephone numbers.

At least in the US, number portability (the ability of a customer to retain his/her number when changing local-exchange service suppliers) is seen as a pre-condition of local-exchange service competition (*Telecommunications Act of 1996*, Sec. 251(b)).

Particularly in the transition period, number portability will be based on remote-call forwarding, direct inward dialling trunks, or other comparable arrangements (Sec. 271). This would have the effect of doubling or trebling the necessary quantity of telephone numbers, in that each subscriber would technically require a unique address with each competitive local-exchange service supplier. Number portability, taken to its limit, will enable a user to take his/her number wherever he/she moves to whichever service provider. In this form, what appears to be a local call can easily turn out to be a long-distance call, being forwarded from a local switch unbeknownst to the calling party.

Telephone company and regulatory responses to number shortages first took the form of contracting the spatial areas covered by an area code. The next wave of solutions is based on the use of multiple area codes for the same geographical area. Under this system, adjoining houses, or even different telephones in the same house, may be assigned different area codes. A third wave of solutions, being discussed in outline form, would increase the number of digits in all telephone numbers. This solution poses significant technical challenges. (Milne, chapter 12, this volume).

Change in the address system of public networks poses serious problems for users, and by extension for regulators. Changes such as overlapping area codes will require additional “work” by calling parties and will accelerate the dissociation of telephone addresses from spatial locations. In advanced forms of number portability, calling parties will lose the ability to distinguish between the relatively cheap local calls and the relatively expensive long-distance calls at the moment of initiating the call. The current US pricing system and the customer routines and expectations associated with it will be destabilised by responses to number shortages. At the present time, most US telephone users pre-pay for local-exchange service on a flat-rate or modified flat-rate basis and post-pay for long-distance service on the basis of usage. The situation resulting from advanced number portability could become so unsatisfactory that a radical change, either toward universal usage-based pricing or toward universal flat-rate pricing, might become necessary. The latter option may be forced if Internet-based voice telephony catches on.

Changes in the addressing system will reduce, if not eliminate, users’ abilities to infer location information from a telephone number. In some cases such as the automated screening and rejection of calls from certain neighbourhoods by commercial organisations (known as “redlining”), the outcome may be positive. However, the number remains a vital piece of access information, despite its disconnection from a spatial referent. What can be predicted is that users will experience a high degree of uncertainty and anxiety in the transition and that regulators and network operators will have to deal with many customer complaints. Changes in addressing systems will also raise new privacy issues. The value of a personal number that a subscriber retains more-or-less for life will be qualitatively higher compared to present numbers. For corporate actors a personal number will be valuable as a crucial piece of “link information” to connect records in different databases. For that reason as well as for purposes of controlling access, network users will also place great value on it. Regulators will be called upon to make policies and/or referee disputes. For calling to persons instead of locations to be fully effective, the whereabouts of users will have to be tracked and such information will have to be stored in network facilities. The terms and conditions of access to these records will also be subject to controversy.

In most, if not all jurisdictions, public policies favour the disclosure of address information. Subscribers are required to pay an additional fee or provide acceptable reasons to keep their names and telephone numbers out of telephone directories. With as many as 50 percent or more of subscribers paying to prevent publication of their access information in a sizeable number of US states including California, this policy bias is likely to come under challenge. It is possible that access information disclosure will cease to be the default police presumptions.

2.3 *Household vs. Individual*

Individuals may directly connect to public telecom networks as sole users, or they may connect as household units. In the former case, there is no intervening social organisation between the user and the network. In the latter case, the rules of the household enable and constrain the individual's access to the network. An individual's interests on whom to communicate with and what information to consume under what conditions, may come into conflict with those of other individuals in the household or with the household's rules. In addition, questions of the household's or subscriber's liability for the actions of individual household members and decisions regarding configuration of the household's interface to the network are likely to increase. These disputes may be alleviated by the above discussed personal telephone numbers, but they will be significant, at least until the new addressing and billing systems are fully in place. It has been customary to conflate household and consumer (perhaps because most scholars and policymakers did not occupy subordinate positions within households), but recent policy controversies have highlighted the need to open the "black box" of the household.

Soon after audiotex services became available in the US, the question of parental liability for portions of the telephone bill reflecting audiotex usage by minors arose (Samarajiva & Mukherjee, 1991). Here, the affected parents denied liability for the high audiotex charges because they did not make the calls and/or the network provider's services had been changed in ways that made parental regulation of network access difficult or impossible. These claims were taken seriously by regulators, legislators, and even by the Local Exchange Companies (LECs). Disconnection of complainants from the network, at least with respect to local telephony, was generally prohibited and various methods of blocking access to audiotex services were devised and offered to parents. In many cases, the LECs forgave the payment due, especially in the case of the first audiotex bill.

The household (or the family) is likely to continue to be a significant factor affecting consumer access to the public network in the foreseeable future. The dependence of minor children on their parents and the persistence of collective living arrangements due to psychological and economic benefits are likely to counter-balance industry initiatives in the areas of personal telecom numbers and devices tending to reduce the importance of collective and stationary access points to the network. As network access becomes more important to children, especially teenagers, parents will seek ways to control that access. The network can be configured to assist parents (default blocking of the majority of network services) or to assist teenagers (non-availability of blocking, or blocking on request, or for fees). Incentives of network providers may lead them in either direction: the former because parents are present subscribers and capable of exerting political pressure; the latter because teenagers are heavy spenders and are

future subscribers. Parents are likely to demand intervention in various forms, as they have already done regarding audiotex, chat-line and online access.

Indeed technological and legislative responses have already emerged. Solutions involving voluntary deployment of technologies that may be utilised by users to screen out or block objectionable online messages are being advocated by legislators and industry as alternatives or supplements to legal measures. An industry alliance including IBM, Microsoft, AT&T, MCI, America Online, Netscape Communications, Time Warner and Viacom has been formed to create standards for this purpose. Computer programs such as SurfWatch and Net Nanny are currently available to allow individuals to monitor and block access to undesired services identifiable by targeted phrases, electronic addresses or other identifying characteristics (Quittner 1995). The purely legislative responses are discussed below.

Increasingly, public telecom networks do not present a “one-size-fits-all” interface to households. Services such as call-waiting, speed-dialling, and calling number identification (CLID) blocking change the configuration of the network as experienced by different households. Some services such as CLID have uniform effects on all households, but most add-on services require affirmative consent and payment (in most cases) by households. Once the CLID software has been installed on the network switch, all calling parties will have their numbers transmitted whether or not they subscribe to the service. However, households have the choice of installing a CLID display device and subscribing to CLID service and various number-delivery blocking options. Current policy is blind as to the manner in which these decisions are taken. It is possible that the subscriber’s decision reflects the common “will” of the members of the household. It is also possible that it does not. For example, an abusive spouse intent on isolating his or her victim may subscribe to CLID to monitor incoming calls. The numbers stored in the display device may be used as “evidence” of transgression by the victim or the abuser may call the recorded numbers to threaten parties communicating with the victim. Using other features of “call management” software, the abusive spouse may institute a permanent blockade of incoming calls from certain numbers, such as the victim’s friends, relatives and social-service agencies.

2.4 Virtual Muggings

Public spaces have never been completely safe. Given that potential for serendipitous encounters is an essential ingredient of publicness, absolute safety can never be guaranteed. However, a public space, proximate or virtual, may have some level of safeguards for persons frequenting it. The “old” telephone network had low safeguards against virtual muggings in the form of obscene and harassing calls. While these actions were criminalized by statute, there was no way to identify a perpetrator who would make only one illegal local call to a victim. Tracing of calls was initiated in response to customer complaints fitting certain pre-set parameters. In fact, most violations of the law prohibiting obscene and harassing calls went undetected and unpunished.

The significance of virtual muggings on upgraded telecom networks increases because of the availability of higher technical capabilities and because users spend more time on the network. For example, depriving a person of sleep is much easier with a redial button or an Automatic Dialling and Announcement Device (ADAD) than when the harasser had to repeatedly dial the numbers through the night. Some technical

solutions proposed for these problems such as CLID result in widespread harm to law-abiding users of the system. They also suffer from technical and regulatory limitations such as non-delivery of numbers from pay-phones and from locations where number-blocking is in place. Other technical solutions such as “Call Trace” and “Call Block” can address the problem more effectively. Call Trace is in effect an automation of the function of a conventional Annoyance Call Bureau. Upon receiving an obscene or harassing call, a user may activate a trace of the offending call. The information is stored in the network’s equipment and may only be retrieved by law-enforcement authorities in response to a legitimate complaint. In the event the user does not wish to initiate a criminal investigation but merely wishes to prevent recurrence, Call Block may be activated, even without knowledge of the number of the offending caller. The user’s phone will not ring for calls originating from the blocked number.

Regulators may no longer be able to ignore matters such as the handling of obscene and harassing calls. As many regulators found to their surprise in the US CLID debates changes affecting the everyday use of the network can arouse much passion and absorb large amounts of regulatory resources. The installation of technical remedies to problems can in many cases create new problems of their own. For example, Call Block can prevent illegal calls, but it can also assist abusive spouses as discussed above. Regulators will be called upon to weigh and balance the competing interests at play.

3.0 Market Issues

The emerging customised mass production economy places great weight on relationships – within the production chain, and between producers and customers. Reliance on one-time transactions is being increasingly superseded by ongoing customer relationships. Transactions are defined as interactions that result in exchange of value. Relationships are defined as iterated interactions or transactions between the same parties. Maintaining relationships with spatially separated customers requires use of telecom networks. It is likely that the bulk of telecom network revenues will come from the provision of facilities for the maintenance of customer relationships, in the same way that a major part of US Postal Service revenues are derived from the provision of bulk mailing services to corporations.

The efficacy of telecom networks as media for the building and maintenance of customer relationships, including persuasive and information seeking activities prior to transactions, the completion of actual transactions, including payment, and in some cases the actual delivery of the purchased item, depends on customers’ willingness to change from old, established ways of doing business and to adopt new ways. As the mixed success of new communication services indicates, this is not an easy task. There is considerable uncertainty on the factors determining the take-up of new communication services. It is possible to identify trust and privacy as necessary conditions for the success of interactive systems as markets.

3.1 Relationships and Trust

Relationships require both parties to know about each other. When small-scale supply of services predominated, proprietors and/or employees of service firms knew individual customers and their preferences regarding a particular service. Indeed, many service-provision activities necessitate relationships with customers. As supply expanded in scale

and numbers of customers and employees grew large, relationships weakened. However, with increasing use of information-communication technologies, it has again become feasible to “know” customers and their preferences. It is of course debatable whether this constitutes knowing, in the sense of one human dialogically engaging with another. Further, this knowing is asymmetrical in two ways. First, the firm knows about the customer, but the customer does not have equivalent information about the firm. Second, the firm in most cases extracts TGI from the customer more-or-less involuntarily, while the customer has, for the most part, to rely on advertising and other persuasive information disseminated by the firm. The degree of involuntariness ranges from the high end of TGI extraction by franchised monopoly firms (e.g., most local-exchange telephone companies) to the low end of competitive firms extracting TGI through point-of-sale routines that require customers to actively resist the extraction of personal information (e.g., collection of telephone numbers for cash transactions by Radio Shack). The value of customer information, particularly TGI, leads firms to combine goods and services (e.g., cars with warranties and service contracts) and convert discrete service transactions into relationships (e.g., frequent-travel programs), in both cases, generating continuing streams of TGI for company databases and consolidating relationships.

Kenneth Arrow's (1975, p. 24) assertion that “virtually every commercial transaction has within itself an element of trust, certainly any transaction conducted over a period of time” suggests that trust is an essential ingredient of a commercial relationship. Giddens (1990, p. 121), in a discussion of trust in interpersonal contexts, states that “relationships are ties based upon trust, where trust is not pre-given but worked upon, and where the work involved means *a mutual process of self-disclosure..*” (author's emphasis). Both appear to imply that a relationship could not exist without a modicum of trust. It is true that trust-related attitudes are crucial elements of relationships and that trust is the foundation of stable, productive relationships. However, it is misleading to infer that all relationships are based upon trust. The corollary to Giddens' claim that trust has to be worked upon is that the work may not be undertaken or may fail; that instead of trust, mistrust or angst may result. While Arrow's claim may hold in an idealised competitive environment, customer relationships marked by mistrust and angst cannot be ruled out in the presence of information asymmetries, spatial monopolies and barriers to exit faced by parties, particularly consumers.

Giddens distinguishes between interpersonal and system trust. He defines trust as “confidence in the reliability of a person or system, regarding a given set of outcomes or events, where that confidence expresses faith in the probity or love of another, or in the correctness of abstract principles (technical knowledge).” Trust derives from faith in the reliability of a person or system in the face of contingent outcomes. The primary condition that creates a need for trust, according to Giddens, is lack of full information, generally associated with a person who is separated in time and space or a system whose workings are not fully known and understood. Given perfect information, faith and trust would be superfluous. Lacking complete information about a system, a person who has to use it has to develop a trust-related attitude toward the system. This can range from complete trust through mistrust to angst. Individuals who interact and transact with complex business organisations lack full information about their workings and have to rely on trust. When such interactions and transactions are mediated by interactive systems, trust is even more important. Given the documented importance of proximity,

co-presence and talk, particularly for contextualising interactions and building relationships, interactive systems that minimise or eliminate these factors heighten the need for trust. Individuals lack information both about the business organisation and about the mediating interactive system. Businesses also lack information about their current or prospective customers. However, businesses have an alternative to trust. They can obtain more information through coercive surveillance, overt or covert.

Trust is dynamically generated. It has to be “worked on.” Trust, both in persons and systems, has strong aspects of mutuality. In interpersonal relationships, one party’s actions, particularly self-disclosure or lack thereof, can reinforce, diminish or destroy the other party’s trust. This claim can be extended with care to customer relationships. While the symmetry suggested by “opening out of the individual to the other” and “mutual process of self-disclosure” would be unrealistic in customer relationships, some aspects of trust-building behaviour such as absence of coercion in making and receiving disclosures, non-release of customer information to third parties without explicit permission, and a degree of disclosure, albeit non-symmetrical, may be expected from a commercial organisation.

These aspects overlap with the above stated definition of privacy as “the capability to explicitly or implicitly negotiate boundary conditions of social relations.” Privacy is situational and relation-specific. In some contexts, a person will voluntarily yield highly personal information and will not consider that release, by itself, a diminution of privacy. In other contexts, the most mundane information will be guarded with great care. The same applies to the reception of information. Privacy is a precondition for trust – an attitude developed on the basis of situational or experiential factors. Trust affects privacy. A user’s trust about the information practices of a system is likely to enable consensual surveillance, which can further enhance trust. The resultant spiral will lead to stable and productive customer relationships.

Conversely, where a system engages in coercive surveillance, mistrust and angst are likely to result. Customer mistrust or angst about the information practices of a system is likely to lead to reduced release of information, tolerance of misinformation, release of disinformation and greater resistance to receipt of information from the system. In the face of the resultant information problems, the system can either increase reliance on trust or on coercive surveillance. The former action is likely to be counterproductive in the short-term unless the underlying mistrust or angst on the part of the customer is removed. The latter action, if known to the consumer, will further decrease trust, giving rise to a spiral of mistrust. If the consumer cannot exit the system, the result will be a pathological customer relationship. Alienated customers and ex-customers can communicate their experiences to current and potential customers, decreasing their trust in turn – a decidedly undesirable outcome for a business organisation.

Outcomes can range from stable, productive relationships to pathological relationships. Actual outcomes are likely to have greater or lesser affinities to the two ideal types. The mere fact of mediation by telecom systems does not change the outcome. Telecom systems can be used for consensual as well as coercive surveillance. The conditions under which a commercial organisation will choose to create a trust-conducive environment or take the path of coercive surveillance require independent explanation.

Commercial organisations’ knowledge of the benefits of stable, productive customer relationships and of the costs of pathological relationships, or lack thereof, may

provide a partial explanation. Contemporary commercial practices, which are heavily biased toward coercive surveillance, may be the outcome of ignorance about the results of coercive surveillance and trust-conducive treatment of customers. If this is true, corporate behaviour may be expected to change over time in the direction of fostering trust and privacy. However, if commercial organisations mask coercive surveillance through telecom systems, the current bias toward coercive surveillance may persist. If customers are unaware of surveillance, the destructive spiral leading to pathological customer relationships may be arrested. Long-term and pervasive patterns of coercive surveillance may become entrenched in people's minds and erode current expectations of privacy and trustworthy behaviours.

In addition, little is known about how to create a trust-conducive environment based on telecom systems. Trust in abstract systems depends on the "access points" or interfaces of the systems. Assuming that most contact with abstract systems occurs in the form of interactions with experts or their representatives at the access points, Giddens argues that system trust depends on the demeanour of system representatives such as doctors or airline cabin crews. By their very nature, telecom systems minimise routine co-present interactions with humans representing the system. The public's non-volatile and growing concern about privacy, particularly in relation to corporations and telecom systems, appears to suggest that business organisations are failing to gain trust, and indeed are engaging in practices that lead to mistrust and angst among consumers.

The above discussion presupposes a direct relationship between a commercial organisation and a customer, mediated by a telecom system controlled by the commercial entity. The prognosis for trust and privacy may be better where the relationship between the commercial organisation and the customer is mediated by a telecom system controlled by a third party. This scenario is explored below following the development of needed theoretical concepts.

3.2 Telecom Networks as Meta-audiences

Attention has always been scarce. However, the scarcity and value of attention are highlighted because of expansion of electronically mediated forms of communication accelerated by rapid technological and economic changes. Herbert Simon has stated that "a wealth of information creates poverty of attention and a need to allocate that attention efficiently among the overabundance of information resources that might consume it" (Varian 1995, p. 200). Attention is a precondition for the constitution of interactions or transactions, and, thereby, of relationships. Attention, once obtained, can be utilised for different forms of persuasion. If the persuasion is effective, transactions and relationships can occur.

In a complex economy, attention must be produced and reproduced on an industrial scale. Production of the attention of multiple individuals, not necessarily gathered in one proximate space or at one time, is described as an audience in relation to books, radio and television. An audience may be conceptualised in two primary ways. First, it may be seen as an object that is measured, bartered and sold. Political economists tend to favour this conception (Melody 1973; Smythe 1977; Owen & Wildman 1992). Second, it can be seen as a collectivity of agents who create meaning from media content. Cultural-studies scholars tend to favour this conception. This analysis uses the politico-

economic conceptualisation, while acknowledging the volition of audience members and the relative openness of the meaning-making process.

Technological forms of storing and retrieving information underlie production and reproduction of modern audiences that go beyond the root meaning of an auditory collective. Different technological forms yield different structures within which agents make meaning. Given the proliferation of technologically retrievable messages and channels and the emergence of advanced telecom capabilities, it is useful to differentiate among three meanings hitherto included in the term, audience.

1. An audience is defined as the persons attending to a specific message. This is the core meaning of audience, but previous scholarly and lay usage has been broader. Those attending to a message need not reach a common understanding, nor does attention have to be efficacious from the communicator's perspective.
2. A meso-audience is defined as persons likely to attend to a class of messages. A "daypart" such as the sports audience, is an example. There is no presumption that all those within a meso-audience will end up in the audiences intended by those who produced the meso-audience. The more effective the meso-audience production process is, the greater the probability of that outcome. However, the inherent indeterminacy of meaning making precludes complete success.
3. A meta-audience is defined as that from which meso-audiences and audiences may be produced. Usage such as "the audience for Channel Six" or the "television audience" would fall within this definition. Persons connected to the Internet would be another example.

The threefold distinction allows the different institutions and incentives associated with each to be identified and analysed. Meta-audiences, meso-audiences and audiences are produced and reproduced with effort. They are fluid and ephemeral. Network operators such as telephone companies are primarily engaged in the assembly of meta-audiences. When AT&T prepares and markets directories of its subscribers organised according to their 800 number usage, it is engaged in the assembly of meso-audiences. When a direct-marketing company utilises such directories in its marketing campaigns, it is engaged in the assembly of audiences. Incentives in terms of attention gaining, surveillance, and relationship building and maintenance differ at each level.

Producing and reproducing media audiences has never been easy. In addition to attention consuming activities such as work, interpersonal relations and leisure, a television-audience producer previously had to compete with a handful of other networks/stations in pre-cable United States (and with fewer rivals in other countries). The difficulty increased with the entry of cable and direct-broadcast satellite channels, and by an order of magnitude with the wide range of information and activities available on interactive systems such as the Internet. On one hand, producers of audiences struggle to assemble and hold audiences. On the other, audience members struggle to cope with the plethora of objects competing for their attention. This chapter focuses on the former.

A limited set of devices is used in assembling an audience for a television program: the human attraction to stories, continuity of narratives presented in instalments, "hooks" at the end and at critical points of the instalment, stars, scheduling to optimise flow from one audience to another, regular scheduling (daily or weekly), teasers and advertisements, creation of excitement in other media around issues such as "who shot

J.R.?,” and so on. Only some of these devices pertain to a discrete message and its audience. Others have to do with the channel or network and daypart. Meta-audiences are produced by devices intended to draw people to the channel or network; meso-audiences by those for dayparts; and audiences proper by those for specific programs. To be precise, programs are devices for assembling second-level meso-audiences, that then allow the creation of audiences for advertisements. However, depending on the level of analysis, programs with embedded advertisements (overt or covert, as with product placements) can be taken to be the focus of audience attention.

Many of these tried and tested devices are ineffective with advanced telecom systems, here defined as media systems allowing potential real-time interactivity within the same medium. This definition includes contemporary and upgraded public telecom networks but excludes one-way media such as radio that allow interaction via telephone and print-on-paper-via-mail media such as magazines that allow for interaction via telephone, e-mail, etc. Actual real-time interaction is not necessary, nor is symmetry of information flows. Ability to complete transactions including payment may be included, though not essential. While the conceptual framework can usefully be applied to hybrid media such as television shopping channels made up of television, telephone and credit-card technologies, newspapers that utilise print, voice-mail and/or telephony, and talk radio that uses radio and telephony, only pure interactive systems will be addressed here.

Two ideal types may be identified within interactive systems. The first is designed to sell information and/or communication capabilities to subscribers. Here, the revenue stream is dominated by subscriber payments. Online information systems such as Lexis/Nexis and standard online services such as CompuServe are examples. An advanced telecom system designed to sell information to subscribers can adopt one of two main pricing schemes: it can sell on the basis of usage or it can utilise some form of flat-rate pricing. The former requires fine-grained surveillance. The latter requires less usage tracking, but subscribers may believe that surveillance takes place. Both modes take information, not attention, to be the scarce commodity. The intellectual-property and privacy implications of systems designed to sell information are discussed below.

In the second ideal type, a system operator sells access to a meta-audience, “universal” or otherwise. Universal is defined as inclusive of all or most households or persons in a spatially defined market. Vendors purchase access to the meta-audience as an input to the process of producing meso-audiences and audiences. Here, payments from vendors including advertisers dominate the revenue stream. The US model of commercial television broadcasting is a non-interactive example. The design of UBI, the Québec interactive system currently under construction, is an interactive exemplar (for details, see Samarajiva, forthcoming).

A system of the second type must attract and retain subscribers and induce them to use the services provided by vendors. In other words, the system operator must enable vendors to produce and reproduce meso-audiences and audiences from the meta-audience. Depending on the concrete conditions affecting consumers, the ways in which these objectives may be achieved differ. Where consumers have few alternatives in terms of allocating attention, the meta-audience producer’s task is relatively easy. Where this is not the case, considerable effort, including measures to ensure privacy and build trust, is required.

Operators of advanced telecom systems of the second type do not necessarily have to produce universal meta-audiences. They can choose to produce niche meta-audiences. Here, the dynamics of audience production are less favourable to trust and privacy than with universal meta-audiences. Moreover, niche meta-audiences and meso-audiences tend to be indistinguishable, in that the system operator must provide some reason for a sub-set of consumers to allocate their attention to one niche system instead of another. In addition, first-comer advantages and network externalities that are considerable in interactive systems (and associated services such as payment systems) make the universal-coverage meta-audiences more likely.

A system operator seeking to produce a universal meta-audience is compelled to create a trust-conducive environment. Otherwise, it would not be possible to attract almost all the members of a potential meta-audience to the system, or to enable the production and reproduction of audiences and meso-audiences therefrom. A trust-conducive environment, by itself, will not yield a universal meta-audience. However, given the ability of even small groups of privacy- and trust-sensitive members of the potential meta-audience to prevent universality being achieved, such an environment is a necessary condition.

A trust-conducive environment requires trustworthy and privacy-friendly behaviours from the system operator as well as the vendors using the system to build and maintain customer relationships. As a result, the system operator is likely to cajole and even coerce vendors to cooperate in building and maintaining a trust-conducive environment. Given the incentives all commercial organisations have to build and maintain stable, productive relationships with customers (discussed above) and the difficulties of engaging in covert coercive surveillance on an interactive system designed and controlled by a third party, vendors are likely to cooperate.

3.3 *Intellectual Property*

An advanced telecom network serves as a marketplace for the buying and selling of all kinds of goods and services, including, but not limited to information. However, with all goods and services, except information and a limited set of services such as access to computer games, the transaction cannot be completed on the network. Delivery of the purchased item has to take place off the network. Consequently, considerable attention is being paid to the development of intellectual property regimes enforceable on interactive networks.

At the technical level, efforts appear to be focused on methods such as “data metering,” described as follows:

The concept is simple: instead of charging a flat fee for a software program, or an hourly fee for access to a database, data metering allows companies to charge per *use*. . . . Think of this metering device as an electric meter that keeps track of the flow of data into your computer and bills you accordingly. . . . With either system [referring to two commercial systems in development], a user can transfer money onto the meter by providing a credit card number When a user requests a program off a CD-ROM or an online database, the meter subtracts the appropriate amount . . . and downloads and decrypts the data. Downloaded programs may be set so that they live for only a few days or uses (Steinberg 1995).

These methods are unlikely to achieve easy success because they are based on extremely fine-grained surveillance that is inimical to trusting commercial relationships. For these mechanisms to take hold, the database providers would have to hold monopolies over certain kinds of information or have established trusting customer relations and consensual surveillance. At the legal level, it appears that national and international initiatives, the latter embedded in trade law, are being built on the shaky foundations of built-in and fine-grained surveillance and the assumption that information, not attention, is the scarce commodity (Samuelson 1996).

4.0 Expression Issues

Many observers have advocated the common-carrier doctrine as a sound basis for addressing the policy issues related to expression of ideas over public telecom networks. Over time, the basic tenets of common carriage – just and reasonable prices and no discrimination – have been supplemented by the separation of content from conduit and the principle that communication common carriers cannot exercise editorial control of what they carry (*National Association of Broadcasters v. FCC* 1984, p. 1203). From this, some conclude that telecom common carriers are not liable for the content of messages carried (Kapor & Weitzner 1993). The common-carriage doctrine appears attractive to telecom regulators because public network operators have historically been treated as common carriers and because it shields regulators from the messy business of regulating content.

With the emergence of audiotex and chat-line services exemplifying the blurring of the distinction between point-to-point and point-to-multipoint communication, government regulation of pornography was extended to telecom, eroding the principle that common carriers have no control over, or liability for, content. In addition, *Chesapeake & Potomac Telephone Co. v. US* (1993) and a series of similarly decided cases that struck down line-of-business restrictions on common carriers on the basis of the First Amendment eroded the principle further.

The US Supreme Court in *Sable v. FCC* (1989) found unconstitutional an amendment to Section 223 of the *Communication Act* that banned all indecent commercial telephone messages within Washington, DC or in interstate or foreign communication, but upheld the ban on obscene commercial messages. The ban on commercial indecency was found to be overbroad. The decision affirmed the constitutionality of other means of preventing access by minors to indecent content including credit-card, access-code and scrambling rules. These principles have now been codified with broad applicability in the US *Telecommunications Act of 1996* (Section 502).

The debate over obscene and indecent commercial telephone services prefigured policy debates regarding regulation of public networks including the Internet. *Sable* was the first time the highest court accepted the principle that a telecom common carrier may be held accountable for content (subject to good-faith defences, but nevertheless accountable). Given the large number of content providers on telecom networks, including online systems, the telcos tend to be the most realistic targets of regulation and litigation. This liability causes telcos to reject or constrain information services based on judgements of content. In some cases, certain information services are denied access altogether. In others, they are denied billing services or are relegated to certain number

prefixes (or regions of virtual public space), with attendant implications for audience production. The explosion of cross-border audiotex services is one of the outcomes of efforts to regulate audiotex content.

Depending on the constitutionality of prior restraint on expression by government, different policy solutions may be devised. In the US, government has sought to create conditions wherein private entities operating public networks will regulate content, circumventing constitutional prohibitions. In other countries, government may seek to regulate content directly. US experience has shown the existence of a range of methods to regulate content on public networks, including:

1. Prior restraint of expression, by government or by network operators.
2. Criminalisation of certain forms of expression, resulting in prosecution after publication.
3. Screening of users to ensure that certain services are not used by members of protected classes.
4. Segregation of information services through devices such as different prefixes and the regulation of access by protected classes of users to certain classes of services.
5. Labelling of messages and services in ways that enable users to make informed decisions regarding access, and enable persons in authority to prevent access to certain messages and services by members of protected classes.

Each of these methods has different strengths and weaknesses. Generally, solutions 1. and 2. are problematic in democratic societies and are difficult to enforce in the context of the existence of a multitude of information providers and the “borderless” nature of contemporary public telecom networks. Solution 3. poses serious privacy problems. If screening of users is to be effective, it is necessary to monitor information use behaviours of all users, combine those records with access and identification information and store at least a portion of the collected information. By elimination, only options 4. and 5. remain within the pale. Not all configurations of these methods minimise damage to democratic values and entrepreneurial freedom. However, there is experience that regulators can draw upon to devise remedies that minimise harm.

In addition to the more controversial content regulation provisions, the *Telecommunications Act of 1996* encourages the use of technological solutions for controlling access via public telecom networks to arguably objectionable content. The Federal Communications Commission and other regulatory agencies are authorised to describe (but not enforce) “reasonable, effective and appropriate measures” for restricting access by minors. Persons acting to restrict access are shielded from prosecution (Section 502). In addition, the new Act protects from civil suit individuals and access providers acting in good-faith to block or screen access to material the access provider or users consider “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.” Access providers providing technological means to “filter, screen, allow, or disallow content; pick, choose, analyse, or digest content; or transmit, receive, display, forward, cache, search, subset, organise, reorganise, or translate content” will not be treated as publishers

or speakers (Section 230), thereby retaining immunity from liability for content, among other things.

The Act is silent on the question of “tagging” information provided over public networks that seems necessary for blocking and screening mechanisms to be fully effective. It is questionable whether a uniform “tagging” standard, even if established outside government auspices, can be “voluntary.” Even if such a standard is not mandated by government, its effectiveness would rest on a strong expectation by legislators, as well as by users, of adherence by network providers. Otherwise, blocking and screening efforts would be futile because many, if not most, of the content providers of arguably objectionable material have an incentive not to “tag” themselves with the signals or codes indicating the nature of their service, because it would result in being automatically excluded from a large part of their potential market.

In fact, the technological option would require the development of one or more private mechanisms for establishing ratings or tags (e.g., a network content ratings board) and for enforcement, unless tags are directly applied by a ratings board or network provider to the content of various online service providers. Given due-process concerns, an appeals process would most likely be warranted. Thus, a technological screening regime would necessitate a private regulatory regime. For those who do not adopt the tag standard, possible actions may include a potentially embarrassing “unrated” or “unapproved” tag. However, the embarrassment of receiving a “negative” rating may not be as strict a penalty as affixation of a tag or rating that permits users to automatically block that particular service, particularly if the service is adult-oriented. Thus, it appears that participating networks will have to make the adoption of an established “tagging” standard by online service providers compulsory for the technological solution to work. In addition, the practicability of a rating system based on tags rests on the assumption of a limited number of information producers (as in the US motion picture industry and the music industry which serve as precedents). This assumption does not hold for network information provision activities, though it may hold for network access.

5.0 Concluding Comments

This brief survey has covered a range of novel regulatory issues likely to emerge as investments in advanced telecom networks, also described as public information infrastructures and information superhighways, accelerate. Contrary to the prognostications of regulatory obsolescence, this analysis argues that new issues pertaining to usage of telecom services will demand the attention of telecom regulators. Conventional economic regulation relied on a theoretical framework, albeit one that was rarely made explicit and even more rarely justified at the level of fundamental assumptions. Whatever its faults, the economic framework focused attention on a limited number of aspects of the object of regulation. It is hoped that the theoretical frameworks of virtual public space, trusting relationships, and audiences will serve a similar function for future issues relating to usage on advanced telecom networks.

Endnotes

¹ The author is grateful to Peter Shields and Scott Potter for early discussions on some ideas presented here; and to the Institute of Public Utilities at the Michigan State University, for opportunities to try them out.