Fordham Law Review

Volume 64 | Issue 3 Article 6

1995

Privacy and Communications Networks

Joseph A. Post

Privacy and Communications Networks

Cover Page Footnote

The author represented New York Telephone Company in proceedings before the New York State Public Service Commission relating to some of the subjects covered herein. Any views expressed in this discussion are, of course, the author's own.

PRIVACY AND COMMUNICATIONS NETWORKS

*Joseph A. Post**

INTRODUCTION

From the earliest days of its recognition as a legal concept, privacy has been considered to have two aspects: the right to control the disclosure of personal information, and the right to be free of intrusions into one's "personal space." Both of these interests are affected in varying ways by communications networks such as those that will comprise the information superhighway. On the one hand, the very purpose of such networks is to deliver information, and the more effective a network is for that purpose, the greater is the potential it creates for the transmission, capture, storage, and use of "private" information. It is overly simplistic, however, to regard communication networks as mere threats to privacy whose development must stringently be controlled. The more "intelligent" a network is, the greater the capabilities it will confer on users to protect themselves from unwanted intrusions by controlling both inward and outward flows of information. In short, the same advances in communications technology that may threaten some privacy interests may also advance others. Legislators, regulators, and market mechanisms will all play roles in achieving some sort of a balance between these disparate and sometimes conflicting interests.

"Caller ID" service provides a paradigmatic case of such conflicts of interest, and it will therefore be worthwhile to consider the service in some detail before discussing more general issues related to privacy and communications networks. As in the following section of this Report dealing with universal service issues, the premise of this discussion is that a consideration of legal and regulatory questions that have arisen in connection with existing communications networks will provide some insight into the issues that are likely to arise in the future as technology evolves, new infrastructure is deployed, and a wide variety of new services come to be offered.

I. A PARADIGMATIC CASE: CALLER ID

In the early days of telephony, most calls were mediated by human operators, and the custom was for the operator to identify the calling party to the person being called. With the advent of direct dialing, the role of the operator diminished, and callers gained the ability to make calls without disclosing who they were or where they were calling from. Perhaps as a vestige of the older pattern, however, common

* The author represented New York Telephone Company in proceedings before the New York State Public Service Commission relating to Caller ID and in a variety of other proceedings relating to some of the subjects covered herein. Any views expressed in this discussion are, of course, the author's own.

opinion continued to support the idea that the caller should be identified. In a recent paper, James Katz assembled extracts from several etiquette books supporting the existence of this custom[477] and noted that "[n]either is this opinion a recent one; in fact it has been a bulwark of social practice throughout, and before, this century."[478] Nevertheless, whatever etiquette may dictate, the fact is that, in most cases, callers can conceal their identity, or at least the number of the telephone line from which they are calling.

In recent years, telephone companies have been deploying a new technology known as common channel signaling. Such technology essentially entails the delivery of information related to the call ("signaling" information) on a separate set of communications paths from those used to transport the call itself. Common channel signaling technology creates a number of network efficiencies, but it has also led to the development of new telecommunications services that utilize the more detailed signaling information that can be delivered over common channel signaling networks. One such service is Caller ID, which allows the called party to see the telephone number of the line from which a call originates. The number is shown on a small display device that can be purchased separately or as part of an integrated telephone set. The number appears on the display between the first and second rings.

As telephone companies began introducing Caller ID in the late 1980s, a number of groups objected to the perceived invasion of their privacy that the service represented, and state regulatory bodies held numerous hearings on privacy questions raised by Caller ID.[479] The interests canvassed in these cases were wide-ranging. On the positive side, Caller ID gave those who used the service greater control over incoming calls and over the manner in which they were handled. Small businesses pointed to the potential use of Caller ID for verifying caller identity, preventing fraud, and otherwise facilitating telephone transactions with customers. Many claimed that the deployment of the service deterred annoying, threatening, or obscene telephone calls, or at least facilitated the identification and apprehension of those who

477. James E. Katz, Sociological Perspectives on Caller-ID Privacy 5-7 (Dec. 20, 1989) (Bell Communications Research Tech. Mem. TM-ARH-015905).

478. *Id.* at 6.

479. *See, e.g.*, Opinion and Order Authorizing Caller ID Service 52-53, Case 91-C-0428, Opinion No. 92-5 (N.Y. Pub. Serv. Comm'n April 9, 1992) (addressing New York's decision to allow Caller ID devices); *see also Re* Southern New England Tel. Co., 134 Pub. Util. Rep. (PUR) 4th 124, 128-30 (Conn. Dep't Pub. Util. Control 1992) (discussing research on the consumer demand of Caller ID in Connecticut); *Re* US West Communications, Inc., 131 Pub. Util. Rep. (PUR) 4th 486, 500-04 (Ariz. Corp. Comm'n 1992) (expressing Arizona's concern with "the privacy implications resulting from approval of . . . Caller ID"); *Re* Diamond State Tel. Co., 121 Pub. Util. Rep. (PUR) 4th 317, 329-32 (Del. Pub. Serv. Comm'n 1991) (regarding Delaware's Caller ID concerns).

made such calls. Emergency service providers testified to the use of the service in identifying emergency callers.

Those opposed to Caller ID testified about the potential use of the service by businesses to assemble telemarketing lists, the interests of telephone "hotlines" (e.g., suicide prevention lines) in being able to give their clients confidence that they could call anonymously, the interests of law enforcement agencies in preventing subjects of investigations from identifying the source of calls from undercover agents, the interests of victims of domestic violence in being able to take refuge in shelters and to call their spouses or children without disclosing their whereabouts, and the interest of doctors, teachers, and other professionals in being able to call their patients, pupils, or clients from their homes without disclosing their home telephone numbers.

Masses of evidence were produced concerning the importance of each of these interests, the likely impact of Caller ID on such interests, and the existence of alternative ways of advancing or protecting them if the offering of Caller ID was or was not approved.[480] Many of the interests on both sides may properly be characterized as privacy interests. As a general matter, Caller ID may be said to advance one form of privacy by affording its users a way to protect themselves from incoming (telephonic) intrusions, while impacting another form of privacy by allowing the disclosure of assertedly "private" information (i.e., the number of the telephone line that the caller is using).

Different states have reached different conclusions about how the service should be offered.[481] One fairly common solution, adopted in New York, among other states, has been to allow the offering of Caller ID, but to give the caller the ability to "block," or prevent display of the calling number. If the caller exercises this option, the Caller ID subscriber sees the letter "P" or the word "PRIVATE" on the display device. It might be thought that this option renders the service valueless, but the appearance of the "P" or "PRIVATE" on the Caller ID device itself conveys information (i.e., the caller's choice to use a "blocking" option), that the subscriber may want to take into account in deciding whether to answer the call or how to handle it. Although the ultimate merits of this solution can be debated, it is at least one

480. The evidentiary records that were assembled in these cases are far too detailed to summarize effectively here, but suffice it to say that a number of legitimate interests were identified on both sides of the question.

481. The matter has also been considered by the Federal Communications Commission in the context of interstate calls. *See* Rules and Policies Regarding Calling Number Identification Service-Caller ID, Report and Order and Further Notice of Proposed Rulemaking, 9 F.C.C.R. 1764 (1994).

The FCC's resolution of the issue differed from the decisions reached by a number of states, raising questions related to the desirability of having inconsistent Caller ID requirements for interstate and intrastate calls originating from the same line. *See* Rules and Policies Regarding Calling Number Identification Service—Caller ID, Memorandum Opinion and Order on Reconsideration, Second Report and Order and Third Notice of Proposed Rulemaking, 1995 FCC Lexis 3088 (1995).

that attempts to balance and accommodate the privacy interests on both sides of the equation.

This balance of conflicting interests has been taken perhaps one step further by the offering in some states of a service known as "anonymous call rejection," which allows telephone subscribers to automatically reject calls for which the calling number information has been suppressed. Such calls would be routed to a recording which advises the caller that the called party chooses not to accept "blocked" calls.

There are, perhaps, two lessons to be drawn from the Caller ID experience in considering how privacy issues will and should be handled in the context of the information superhighway. First, there is the danger of framing the issue as a balance between privacy and something else. Both the delivery and the suppression of information simultaneously protect and impair privacy, and the task is to find a way to identify, measure, balance, and accommodate these conflicting interests. Second, there is the need to recognize that technology is both the problem and the solution. Although technology provides new and richer sources of information, it also provides the way for network users to control the flow of such information. The same technology that enables Caller ID also gives callers the means to prevent delivery of their numbers and gives called parties the means to avoid (or reroute, or otherwise manage) unwelcome calls.

Caller ID is but one example of the ways in which privacy issues have been considered in recent years in the context of communications networks and services. Although the precise nature of these issues will change as technology evolves, the general problems—relating to the way in which the generation, transmission, storage, and use of information should be controlled, and who should be entitled to exercise such control—will persist as current networks evolve into the information superhighway of the future. It will therefore be useful to consider some of the issues that have arisen in recent years.[482] A helpful and somewhat more detailed survey of many of these issues can be found in a recent Notice of Inquiry issued by the National Telecommunications and Information Administration.[483]

---

482. Because the purpose of this Report is to identify general types of privacy issues that are likely to be raised in connection with the information superhighway, it does not attempt a detailed restatement of all existing or proposed laws and regulations—state, federal, and international—relating to privacy in telecommunications. The examples discussed below are offered for illustrative purposes only.

No attempt is made to address transnational legal issues related to privacy. For a discussion of some of those issues, see, for example, Robert G. Boehmer & Todd S. Palmer, *The 1992 EC Data Protection Proposal: An Examination of Its Implications for U.S. Business and U.S. Privacy Law*, 31 Am. Bus. L.J. 265 (1993).

483. Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842 (1994) [hereinafter NTIA Notice].

II. Some Privacy Issues Raised by Telecommunications Networks

A. *Who Is Calling?*

One of the most important issues relating to privacy on communications networks is the question of the extent to which a network user should be permitted to communicate or otherwise interact anonymously with another user. Where both parties choose anonymity, no significant privacy issues would seem to be raised. The question, then, is what should happen where less than all of the participants to a communications transaction agree to anonymity.

The issues raised by Caller ID have already been considered. Similar issues have been raised by a different calling number delivery technology known as "Automatic Number Identification," or ANI. ANI is a field of data provided by a telephone company to certain of its customers in connection with the delivery of calls to those customers. In contrast with Caller ID-type signaling data delivered in common channel signaling networks, ANI information is traditionally provided "in band," that is, on the same communications path as the call itself. Since ANI does not depend upon the existence of common channel signaling, it predates such technology by decades.

In general, telephone networks are not designed to transmit ANI information end-to-end along with a call. For that reason the service was never used as the basis for an alternative consumer Caller ID service. Rather, its principal use has been in connection with the "handoff" of calls between carriers. For example, when a long distance telephone call originates on a local telephone company's network, the call must be delivered to the long distance (interexchange) carrier that will carry the call to the called party's local telephone company. The customary billing arrangement for such a call is that the caller is billed only by the interexchange carrier, and not by the local telephone companies at either end of the call.[484] To enable the interexchange carrier to identify the customer to be billed, the originating local telephone company delivers ANI information to that carrier along with the call itself.[485]

In addition to using ANI for billing purposes, some carriers also "repackage" the information, including it as a component of the services they offer to call recipients. For example, the 800-number services offered by some interexchange carriers provide for the optional

484. The local telephone companies bill the interexchange carrier for the service of "originating" or "terminating" the call.

485. The Modification of Final Judgment ("MFJ"), discussed in the following section of this Report, requires Bell Operating Companies to "provide to all interexchange carriers . . . exchange access . . . on an unbundled, tariffed basis, that is equal in type, quality, and price to that provided to AT&T and its affiliates." United States v. AT&T Co., 552 F. Supp. 131, 227 (D.D.C. 1982), *aff'd*, 460 U.S. 1001 (1983). "Exchange access" is defined to include "Automatic Number Identification." *Id.* at 228.

delivery of ANI information to the business subscribing to the 800 number. Businesses that purchase ANI-based services can use ANI for a variety of purposes, including customer identity verification and the facilitation of retail transactions (e.g., the customer's records can automatically be retrieved while the call is being answered). Of course, ANI can also be used to assemble lists of numbers for telemarketing purposes.

Because ANI is conceptually similar to Caller ID (both entail the delivery of the calling number to the party called),[486] it might be thought that similar regulatory frameworks would apply to the two services. In fact, the privacy "solution" adopted by many state commissions in the Caller ID context—caller-directed blocking—cannot be implemented for ANI because existing network technology does not permit the calling party to be given the capability of blocking delivery of in-band ANI information except by blocking the call itself. Moreover, even if it were technologically feasible to do so, allowing callers to block ANI would impair the ability of interexchange carriers to conduct their own billing and collection, thus forcing them to rely on local telephone company-provided billing and collection services. Thus, caller-directed blocking could raise significant issues relating to telecommunications competition.

Accordingly, regulators have focused on an alternative regulatory approach, under which local telephone companies and other carriers may be required to condition the delivery of ANI information on the recipients' agreement to abide by certain restrictions regarding the use to which that information may be put.[487] For example, certain restrictions might be imposed on the use of such information for the purpose of assembling marketing lists. ANI regulation thus affords an alternative model for preventing the abuse of calling party identification information: restricting the *use* of the information rather than preventing its delivery.

B. *User Directories*

Local telephone companies publish "White Pages" directories listing the names, phone numbers, and addresses of their customers. Customers generally have the option of excluding themselves from

486. As a technical matter, Caller ID delivers the telephone number of the line from which the call originates, while ANI delivers the number to which the call is billed. For well over 95% of lines, the two numbers are the same. Some multiline business customers, however, may choose to bill all or some portion of their lines to a single telephone number, even though the lines themselves each have different numbers.

487. *See* Opinion and Order Concerning ANI Terms and Conditions 10, 12-13, Cases 89-C-191 & 90-C-0165, Opinion No. 92-37 (N.Y. Pub. Serv. Comm'n Dec. 3, 1992). As a practical matter, such restrictions would not need to be embodied in separate agreements, but could be included in the carriers' tariffs for their ANI-related services.

such listings by purchasing "non-published number" service. The purchase of this service precludes a customer from appearing in printed directories or in directory assistance databases. Additionally, state law may provide additional restrictions applicable to such customers. For example, the New York Public Service Law provides that "[n]o telegraph corporation or telephone corporation shall sell or offer for sale any names and/or addresses of any of its customers whose listings have been omitted from the telephone company's published directory at the request of the customer."[488]

Given the decision that customers should be allowed to exclude themselves from directories, questions arise as to the appropriate charge to impose for the exercise of the option. Rates currently charged by telephone companies for the service are not necessarily cost-based, but may reflect the diminution of the value of the directory to other customers that is created by a customer's decision to "opt out."[489] Pricing decisions, just like other decisions relating to the terms and conditions on which a privacy-affecting service will be offered, require a sensitive balancing of competing interests in the use of and control over information.[490]

---

488. N.Y. Pub. Serv. Law § 91(5) (McKinney 1989).

489. As the New York Public Service Commission recognized:

> Nonpublished service was first charged for in 1960, at which time it was recognized that a deterrent charge was necessary because nonpublished service was growing rapidly. When this happens, the value of telephone service to all subscribers is diminished since they have difficulty in communicating with subscribers whose telephone numbers are unlisted.

Proceeding on Motion of the Commission as to the Rates, Charges, Rules, Regulations and Classifications of the New York Telephone Company 345, 397, Case 25155 (N.Y. Pub. Serv. Comm'n July 1, 1970).

490. In a September 1991 Revised Statement of Policy on Privacy in Telecommunications, the New York Public Service Commission stated:

> *Considerations of cost, public policy, economics, and technology all bear on the pricing of privacy features, which must be determined case-by-case.* In general, customers choosing a feature that simply protects a pre-existing privacy level against a new service should not be charged for doing so; customers choosing a greater degree of privacy could reasonably be required to pay its costs. These presumptions could be overcome by reasonable showings in particular cases.

Revised Statement of Principles on Privacy in Telecommunications 2, Case 90-C-0075 (N.Y. Pub. Serv. Comm'n Sept. 20, 1991) [hereinafter Revised Statement]. This was but one of eight "principles" or guidelines included in the Revised Statement. The Revised Statement as a whole provides an interesting conceptual framework for reviewing privacy issues, and it is thus worth quoting in more detail:

> 1. *Privacy should be recognized explicitly as an issue to be considered in introducing new telecommunications services. . . .*
>
> 2. *The interest in an open network should be recognized in evaluating alternative means for protecting privacy. . . .* [P]rotective measures should be customer-specific where technically feasible and economically practical, and allowing customers to erect barriers to network access would be preferred to establishing automatic barriers that customers would have to overcome. . . .
>
> 3. *Companies should educate their customers as to the implications for privacy of the services they offer. . . .*

C. *Disclosure of Records Related to the Use of the Network*

A customer's use of a telecommunications network generates a great deal of information. Thus, questions arise as to what restrictions, if any, should be imposed on the use and disclosure of such information. As with calling number information, this issue has been addressed in different contexts under different, and perhaps not entirely consistent, legal and regulatory frameworks. Several of these frameworks are discussed in this subsection.

1. Cable Act

The Cable Communications Policy Act of 1984[491] restricts cable companies' use of information about subscribers' viewing choices. As summarized in the NTIA Notice of Inquiry cited above:

> The 1984 Cable Act precludes cable operators or third parties from monitoring the viewing habits of cable subscribers. Under the subscriber privacy provisions of that Act, cable operators are required to inform their subscribers at the time of entering into a contractual arrangement, and annually thereafter, of the nature of the "personally identifiable information" they collect about subscribers, their data disclosure practices, and subscriber rights to inspect and correct errors in such data. Cable operators are prohibited from using the cable system to collect personally identifiable information about their subscribers, except that which is necessary to render cable service, without subscriber consent, and are generally barred from disclosing such data to third parties without written or electronic consent. Cable operators may sell their mailing lists to third parties

---

4. *People should be permitted to choose among various degrees of privacy protection, with respect to both the outflow of information about themselves and the receipt of incoming intrusions.*
5. *A telephone company offering a new service that compromised current privacy expectations would be obligated to offer a means of restoring the lost degree of privacy unless it showed good cause for not doing so.*
6. *Considerations of cost, public policy, economics, and technology all bear on the pricing of privacy features, which must be determined case-by-case.* In general, customers choosing a feature that simply protects a pre-existing privacy level against a new service should not be charged for doing so; customers choosing a greater degree of privacy could reasonably be required to pay its costs. These presumptions could be overcome by reasonable showings in particular cases.
7. *Unless a subscriber grants informed consent, subscriber-specific information generated by the subscriber's use of a telecommunications service should be used only in connection with rendering or billing for that service or for other goods or services requested by the subscriber. . . .*
8. *Privacy expectations may change over time, requiring, in some instances, changes in telecommunications services. At the same time, changes in telecommunications technology services and markets may lead to changes in customers' privacy expectations.*

Id. at 1-3.

491. 47 U.S.C. §§ 521-613 (1988), amended by Cable Television Consumer Protection and Competition Act of 1992, 47 U.S.C. §§ 521-611 (Supp. V 1993).

> only if they have given their subscribers an opportunity to limit such disclosure, and the disclosure does not reveal the viewing habits or other transactions of the subscriber.
>
> The 1992 Cable Act extended the protections of the 1984 Cable Act to new wire and radio services that may be provided over cable facilities, such as personal communications services (PCS). It also requires cable operators to take actions necessary to prevent unauthorized access to personal information by persons other than the subscriber or cable operator.[492]

Thus, a cable operator's actions with respect to information about their customers is severely restricted.

2. Video Privacy Act

The federal Video Privacy Protection Act of 1988,[493] and similar state laws,[494] limit the dissemination of information relating to video cassette rentals and sales. Such laws arose out of disclosures relating to the possible use of video rental information in the confirmation hearings for Supreme Court Justice-designate Robert Bork, and apparently reflect perceptions that information on video viewing habits are particularly private and personal.

3. ECPA

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the federal Electronic Communications Privacy Act of 1986 (the "ECPA"),[495] imposes certain limitations on the disclosure of information relating to electronic communications.[496] The law reflects interesting dichotomies between the treatment of disclosures to governmental entities on the one hand, and internal use or

---

492. NTIA Notice, *supra* note 483, at 6844 (footnotes omitted) (citing 47 U.S.C. § 551 (Supp. V 1993)).

493. 18 U.S.C. §§ 2710-2711 (1994).

494. *See, e.g.*, N.Y. Gen. Bus. Law §§ 670-675 (McKinney Supp. 1995) ("Video Consumer Privacy Act"); *see also* NTIA Notice, *supra* note 483, at 6844 n.24 (citing examples of state video privacy laws).

495. Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (1968), *as amended by* Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2522, 2701-2711 (1994)).

496. The primary focus of the ECPA is on regulating the interception of communications. "Intercept," as used in the statute, "means the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1994) (emphasis added). Wiretapping and other forms of interception obviously raise another class of privacy concerns, which are not addressed in this section of the Report. Rather, the focus of this section is on the ECPA chapter dealing with access to records of "electronic communications." *Id.* §§ 2701-2711 (1994).

"Electronic communication service" is defined in the ECPA to include "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

disclosure to private third parties on the other.[497] For example, § 2703(c) deals separately with the disclosure of records to "governmental entities" and persons other than governmental entities. Disclosure may be made to governmental entities only under certain limited conditions (e.g., where a warrant is issued).[498] The statute adds, however, that "a provider of electronic communication service or remote computing service *may disclose* a record or other information pertaining to a subscriber to or customer of such service (not including the contents of [such] communications . . .) to any person other than a governmental entity."[499]

4. CPNI

"Customer proprietary network information, or CPNI, encompasses any information about customers' network services and their use of those services that a telephone company possesses because it provides those network services."[500] The FCC has promulgated rules that govern the use of CPNI by Bell Operating Companies, GTE, and AT&T in the marketing by those companies of "enhanced services" and customer premises equipment.[501] The principal, original purpose of such restrictions was to ensure fair competition between (a) local telephone companies that may both provide basic services (and thus have access to CPNI related to those services) and provide enhanced services, and (b) competing enhanced service providers. In effect, the rules seek to prevent telephone companies that generate CPNI through their relationship with basic service customers from gaining an unfair advantage in the marketing of their enhanced services.

In general, the FCC's rules require both competing enhanced service providers and telephone company enhanced services marketing personnel to obtain prior customer authorization before obtaining access to CPNI for customers with more than twenty lines. Telephone company enhanced services personnel may, however, obtain access to

497. Special concerns over *governmental* uses of information are also reflected in the Privacy Act of 1974, which has been amended three times since 1974, and in a number of other federal statutes. *See* 5 U.S.C. § 552a (1994).

498. 18 U.S.C. § 2703(c)(1)(B) (1994).

499. *Id.* § 2703(c)(1)(A) (emphasis added).

500. Additional Comment Sought on Rules Governing Telephone Companies' Use of Customer Proprietary Network Information, 9 F.C.C.R. 1685 (1994) (public notice).

501. *See* California v. FCC, 39 F.3d 919, 923-24 (9th Cir. 1994) (discussing FCC regulation of "enhanced services"), *petition for cert. filed*, 63 U.S.L.W. 3593, 3608 (U.S. Feb. 14, 1995).

Enhanced services are "services, offered over common carrier transmission facilities used in interstate communications, which employ computer processing applications that act on the format, content, code, protocol or similar aspects of the subscriber's transmitted information; provide the subscriber additional, different, or restructured information; or involve subscriber interaction with stored information." 47 C.F.R. § 64.702(a) (1994). "Voicemail," for example, is considered an enhanced service, because it involves customer interaction with stored information.

CPNI for customers having less than twenty lines; competing enhanced service providers must obtain prior customer authorization. Any customer can request that its CPNI be withheld both from competing enhanced service providers and telephone company marketing personnel.

Although developed primarily for purposes related to competition, the CPNI rules do reflect customer privacy concerns. In a March, 1994 release, the FCC solicited comments on "customers' CPNI-related privacy expectations, and whether any changes in [their] rules [were] required to achieve the best balance between customer's privacy interests, competitive equity, and efficiency."[502]

5. New York Public Service Commission Privacy Principles

As noted above, the New York Public Service Commission issued a policy statement on privacy in telecommunications, in the form of a set of eight privacy guidelines or "principles." Principle No. 7 states that: "*Unless a subscriber grants informed consent, subscriber-specific information generated by the subscriber's use of a telecommunications service should be used only in connection with rendering or billing for that service or for other goods or services requested by the subscriber.*"[503] In a petition for reconsideration of an earlier version of the Commission's Statement of Policy, New York Telephone Company stated, in pertinent part:

> Principle No. 7 has potentially broad application, and as adopted it would deter a number of legitimate and beneficial uses of subscriber-specific information. Particularly important in this regard is the use of such information by the Company itself. The Company, like most business enterprises, uses data gathered from its business activities (including "subscriber-specific" information) in efforts to improve and extend the services it offers. For example:
>
> - The Company . . . seeks to provide its customers with the services and features that will best and most economically meet their needs. For example, the Company might review a customer's service records to determine if there is a more economical service option available to the customer . . . .
>
> As drafted, Principle No. 7 would all but preclude such activities, thus hindering, rather than advancing, the interests of the Company's subscribers.[504]

In its September 20, 1991 order revising the Statement of Policy, the Commission addressed this argument as follows:

502. Federal Communications Commission, Public Notice, FCC 94-63 (Mar. 10, 1994).

503. *See supra* note 490.

504. Petition of New York Telephone Company for Reconsideration of the Commission's Statement of Policy Concerning Privacy in Telecommunications 3-4, Case 90-C-0075 (N.Y. Pub. Serv. Comm'n Apr. 22, 1991).

> Nor is any change warranted by the various ways in which New York Telephone says it uses these data.... [I]nsofar as the principle bars use of the information for aggressive telemarketing, that was its intention, and there is no reason to allow a telephone company to do what other marketers may not.
>
> In discouraging aggressive telemarketing, of course, we do not mean to bar a telephone company from using subscriber-specific information to bring to a customer's attention service modifications that might benefit the customer. Because the principles are guidelines and presumptions only, they allow for that flexibility, and a telephone company would not be regarded as having violated an interest protected by Principle No. 7 if it made judicious use of subscriber-specific information in bringing potentially beneficial service modifications to the attention of customers.[505]

These statutes, rules, and principles raise interesting questions about the extent to which the use of "transactional" information related to the use of a communications network should be restricted. Does public policy support a different level of restrictions on the use of such information by service providers themselves, and the disclosure of such information to third parties? Does disclosure to governmental entities raise significantly different concerns than disclosure to private third parties? To what extent should service providers be required to notify customers of their disclosure practices and give customers the right to opt out? Are there particular categories of information which deserve especially stringent levels of protection? These issues will all have to be addressed in the context of new telecommunications technologies.

CONCLUSION

Each of the concerns discussed above is raised, or will be raised in some form, by the information superhighway. Like traditional telephone networks, the superhighway, in whatever form it eventually manifests itself, will generate transactional records containing arguably personal information, will permit anonymous interactions, and will create a vehicle for intrusive and unsolicited commercial solicitation. The statutes, cases, and principles discussed above will provide a starting point for analyzing and resolving such concerns.

505. Revised Statement, *supra* note 490, at 16-17.