

Gina Harrison
Director
Federal Regulatory Relations

1275 Pennsylvania Avenue, N.W., Suite 400
Washington, D.C. 20004
(202) 383-6423

PACIFIC  **TELESIS**
Group-Washington

EX PARTE OR LATE FILED

January 24, 1997

RECEIVED

JAN 24 1997

U.S. DEPARTMENT OF COMMERCE
FEDERAL COMMUNICATIONS COMMISSION

EX PARTE

William F. Caton
Acting Secretary
Federal Communications Commission
Mail Stop 1170
1919 M Street, N.W., Room 222
Washington, D.C. 20554

Dear Mr. Caton:

Re: CPNI, CC Docket No. 96-115

A copy of the attached analysis of privacy issues, and accompanying summary of points, by Privacy & Legislative Associates was sent to the individuals listed below. Please include this material in the above-referenced docket. We are submitting two copies of this notice, in accordance with Section 1.206(a)(1) of the Commission's rules.

Please stamp and return the provided copy to confirm your receipt. Please contact me should you have any questions.

Sincerely yours,



Attachment

cc: L. Atlas
D. Atwood
P. Gallant
R. Keeney
B. Kehoe
A.R. Metzger
G. Teicher

No. of Copies rec'd
List ABCDE

0+1

PRIVACY & LEGISLATIVE ASSOCIATES

1150 CONNECTICUT AVE., N.W., SUITE 700

WASHINGTON, D. C. 20036

202-296-2862

January 23, 1997

A. Richard Metzger, Jr.
Deputy Chief, Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W.
Room 500
Washington, D.C. 20554

Re: Telecommunications Carriers' Use of Customer Proprietary Network Information,
FCC Docket No. 96-115

Dear Mr. Metzger:

Privacy & Legislative Associates, Inc. has authored this analysis of privacy issues relevant in the above-referenced docket.¹ We submit this analysis on behalf of the Pacific Telesis Group.

I. SUMMARY

This submission makes the following three points.

- Customer Proprietary Network Information ("CPNI") contains personal information and is appropriately the subject of privacy concern. The use of CPNI, however, does not pose the same privacy risks as does the use of certain other categories of personal information, such as medical and financial record information. For the reasons discussed below, CPNI is not as "sensitive" as medical or financial or certain other categories of personal information.
- Because CPNI is not as "sensitive" as many other kinds of personal information, it is appropriate that the use and disclosure of CPNI be subject to opt-out rules, as opposed to affirmative consent rules -- opt-in rules -- customarily applied to medical and financial records.

¹ See Appendix A for a description of Privacy & Legislative Associates, Inc.

- The sharing of personal information among affiliated corporations (related by common ownership or control) is customarily permitted, subject to customer notice and opt-out, where the personal information at issue is not highly sensitive.

II. SENSITIVITY OF CPNI

An opt-out process -- customer notice of intended information disclosures and/or uses and an opportunity for the customer to indicate the customer's disapproval of the proposed disclosure and/or use -- is a legitimate, customary and appropriate process when the information at issue is relatively non-sensitive and the disclosure and use at issue do not affect an individual's eligibility for or access to benefits or entitlements.

While no exact formula measures the level of sensitivity of personal information, the following three factors customarily are used to classify or rank the sensitivity of personal information:

- The subject matter to which the information pertains;
- The relationship between the individual about whom the information is collected and the collector of the information ("relational interest"); and
- The actual and potential use of the information.²

² Moreover, sensitivity varies substantially depending upon the individual about whom information is collected. Analyses conducted by Dr. Alan F. Westin of Columbia University and Privacy & Legislative Associates, and based upon surveys conducted by Louis Harris and Associates and commissioned by Equifax, indicate that the public divides into three categories of privacy sensitivity. Approximately 16 percent of the public are "privacy unconcerned" and, for them, there is very little in the way of personal information which they deem to be "sensitive." Another approximately 24 percent of the public can be classified as "privacy fundamentalists" and, for them, almost any personal information is deemed to be quite sensitive. The majority of the American public, approximately 60 percent, can be usefully categorized as "privacy pragmatists." For them, the sensitivity of personal information will vary, depending upon the factors discussed in this submission, as will their tolerance for the disclosure and use of this information. The 1996 Equifax-Harris Consumer Privacy Survey, at 13-14 (1996).

CPNI, as defined in the Telecommunications Act of 1996, consists of:

(A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.³

As such, CPNI is personally identifiable information and its collection, use and disclosure can raise privacy issues. On the other hand, however, CPNI is not as sensitive as other personally identifiable information such as medical record information, financial and credit record information, insurance information, employment performance information and other categories of personal information which provide insight into an individual's performance or condition or provide information regarding sensitive personal relationships.

³ The Telecommunications Act of 1996, Sec. 702, Pub. L. No. 104-104, 110 Stat. 148 (codified at 47 U.S.C. § 222).

A. Subject Matter

The Privacy Working Group of the Clinton Administration's National Information Infrastructure Task Force has addressed the issue of sensitivity of personally identifiable information in its "Principles for Providing and Using Personal Information."⁴ The explanatory commentary to those principles emphasizes that not all personal information is of equal sensitivity. The commentary calls for a "nuanced" approach to crafting privacy protections which take into account a "host of factors," including specifically, the subject matter of the information. Similarly, the National Telecommunications and Information Administration's Report on Privacy and the NII: Safeguarding Telecommunications-Related Personal Information distinguishes among categories of personal information and concludes that information pertaining to health care, political persuasion, sexual matters and orientation, personal finances and Social Security Numbers are "sensitive" information.⁵

Public opinion surveys make clear that the public evaluates the privacy threat posed by personal information by weighing a variety of factors including, in particular, the subject matter of the information. A 1994 survey conducted by Louis Harris and Associates and commissioned by Equifax with Alan Westin as academic advisor, rated the following four types of personal information as most sensitive: (1) health and medical; (2) banking and credit card; (3) insurance; and (4) credit reports. All of these types of personal information share a common element: they reveal information about health or financial status and, when disclosed

⁴ "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, A Report of the Privacy Working Group," (October, 1995) [hereafter, "Report of the Privacy Working Group"].

⁵ U.S. Department of Commerce, National Telecommunications and Information Administration, "Privacy and the NII: Safeguarding Telecommunications-Related Personal Information," (October 1995), at 25 n.98.

without authorization, this kind of personal information customarily has the capacity to embarrass and stigmatize the individual about whom the information is collected.⁶

Health and medical record information, for example, is widely viewed as extraordinarily sensitive.

Medical records often contain intimate personal information. If disclosed to others, this information could cause embarrassment and humiliation... Disclosure of medical information could also damage family relationships, reputation and self-esteem.⁷

CPNI, by contrast, does not contain intimate personal information and, if disclosed to others, poses far less of a risk than health and medical information of resulting in embarrassment, humiliation or stigma. For example, the unauthorized disclosure of medical record information, containing such intimate details as a history of physical or mental illness or a genetic predisposition to a certain disease, can result in humiliation and embarrassment. Similarly, the unauthorized disclosure of financial record information, such as depository records or credit history, can embarrass and stigmatize. The unauthorized disclosure of CPNI, by contrast, does not present nearly the same threat. For example, information about the number of telephones in a residence or whether the customer subscribes to call waiting is highly unlikely to embarrass, humiliate or stigmatize the customer.

B. Relational Interest

Most personal information is not "created" wholly by the individual who is the subject of the information. Instead, personal information customarily arises out of transactions or events which occur in a relationship. In some of these relationships, such as a doctor-patient

⁶ See, Bloustein, "Privacy as an Aspect of Human Dignity," Philosophical Dimensions of Privacy, Shoeman F., Editor (1984) at 176.

⁷ "Privacy Rights in Medical Records," 13 Ford. Urban L.J. 165 (1985).

relationship, a lawyer-client relationship or a banker-depositor relationship, creating and sharing personal information is crucial to establishing a bond of trust which, in turn, is critical to the success of the relationship. In other words, the express or implied promise of privacy and confidentiality attaching to the relationship is viewed as a prerequisite for the success of the relationship.

In calculating the sensitivity of categories of personal information, it is important and customary to evaluate the relational interest in which the information is created and used, including the extent to which there is an existing relationship between the individual about whom information is collected and the information collector; the degree of trust between the individual about whom information is collected and the information collector; and the extent to which there is an expectation that the information will be kept confidential.

Confidentiality in the relationship between a telecommunications carrier and a customer (apart from the content of telephone or telecommunications messages) is not as important as confidentiality is in certain other relationships, such as the doctor-patient relationship. In the doctor-patient relationship, if a patient fears that the doctor will divulge the patient's sensitive medical information, the patient will not repose trust and confidence in the doctor and thus, the patient is less likely to fully and candidly share wide-ranging and intimate personal information.⁸ In the relationship between a customer and a telecommunications carrier, by contrast, it is not imperative or even appropriate that the customer share wide-ranging and intimate personal information. Simply stated, privacy and confidentiality safeguards are not as critical to the success of the telecommunications carrier-customer relationship as they are to the doctor-patient relationship.

⁸ "Confidentiality encourages the unfettered exchange of information between the patient or client and the professional. Such uninhibited discourse is essential to effective treatment or therapy. Under this view of confidentiality, the immunity arising from non-public disclosure of health care information protects the integrity of the relationship by promoting trust between the patient or client and the professional." Turkington, "Legal Protection for the Confidentiality of Health Care Information in Pennsylvania: Patient and Client Access," 32 Vill. L. Rev. 259, 268 (April, 1987).

This view is reflected in the results of a 1993 Louis Harris survey conducted for *Privacy & American Business*. The survey asked the public, "how important is it that businesses have strong privacy policies?" The following categories of services (and relationships) were seen as requiring very strong privacy policies: banks - 72 percent of the public said that strong privacy policies are "very important"; health insurance companies and hospitals and clinics - 71 percent provided this answer; credit card companies - 67 percent provided this answer; life insurance companies - 66 percent provided this answer; and stock brokers and investment firms - 56 percent provided this answer. By contrast, only 53 percent of the American public said that it was "very important" that long distance telephone companies adopt strong privacy policies. This finding is consistent with the view that the American public does not think that the relationship between consumers and telephone companies is the kind of fiduciary relationship that requires or warrants privacy policies in the same way that the relationship with health or financial service providers does.

C. The Purpose for Which CPNI Can Be Used

The third element that is customarily considered in a sensitivity calculation is the extent to which personal information is being used, or could be used, to make significant decisions affecting an individual's access to benefits or entitlements. CPNI is used only to provide telecommunications services to a customer or to market such services to an existing or potential customer. Medical record information, by contrast, can, and does, influence decisions about treatment; about entitlement to health care payment; and about employment decisions, licensing decisions, and numerous other decisions that have a significant impact upon an individual.⁹ Similarly, financial and credit report information can, and does, routinely influence decisions

⁹ See, for example, "Health and Medical Records" in Trubow, Privacy Law and Practice, Matthew Bender and Co. (1991) at 7-3 through 7-5.

about access to credit (and thus, access to goods and services), access to insurance and, in some cases, access to employment and licensing.¹⁰

On the other hand, CPNI is not used to allocate scarce resources or benefits. Indeed, it is difficult even to envision how CPNI could be used to make a significant decision affecting an individual. Instead, CPNI is used to make service decisions regarding a consumer's existing telecommunications services and to apprise consumers of new or enhanced telecommunications products and services. These are not decisions that have a significant or adverse impact upon consumers.

Applying the three criteria customarily used in a sensitivity analysis -- the subject matter of the information; its impact on the relationship in which it was created; and its potential for use in making decisions affecting benefits and entitlements -- it is clear that CPNI is not sensitive personal information in the way that medical or financial record information is sensitive. This does not mean that there is no privacy interest in CPNI or that privacy safeguards should not be attached to CPNI. It does mean, however, that these privacy safeguards should be proportionate to CPNI's privacy sensitivity and risk. A sensitivity analysis of CPNI, therefore, suggests that an opt-out approach -- and not an opt-in approach -- is the preferred and attractive option.

III. OPT-OUT IS CUSTOMARY AND APPROPRIATE

Under an "opt-in" approach, an information holder cannot disclose personally identifiable information unless the individual affirmatively consents to the disclosure. Under an "opt-out" approach, an information holder may disclose personally identifiable information

¹⁰ "For many Americans their credit standing is a significant asset. Their credit reporting file affects their access to home mortgages, car loans and other forms of consumer credit, residential tenancies, employment and even insurance." National Consumer Law Center, Fair Credit Reporting Act, Third Edition (1994) at 29.

unless the individual, after receiving a notice describing the proposed disclosure(s), notifies the holder that the individual does not consent to the disclosure.

An opt-out approach is the customary and appropriate method for obtaining an individual's approval for the use and disclosure of personal information pertaining to the individual when the subject matter of the information is personal, but not highly sensitive; when the information has not been developed in a fiduciary relationship; and when the information is not used, intended to be used or capable of being used to make significant decisions about the individual. For all of these reasons, it is appropriate that the use and disclosure of CPNI be subject to an opt-out procedure.

The notion that an individual should have notice of the collection, maintenance, use and disclosure of his personal information by a recordkeeper and an opportunity, in some manner, to approve the use or disclosure is relatively recent. In 1973, the Advisory Committee on Automated Personal Data Systems ("Advisory Committee"), appointed by the Secretary of Health, Education, and Welfare, proposed the first-ever comprehensive information privacy principles for computerized recordkeeping of personal information.¹¹ The Advisory Committee made five recommendations which have come to be referred to as the "Code of Fair Information Practices." The Advisory Committee's report emphasized that these fair information practice principles should be made applicable only to "administrative personal data systems," i.e., systems using personal information to make decisions affecting an individual's access to benefits or entitlements.¹² When personal information is used for other purposes,

¹¹ See, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare (1973), in Records, Computers and the Rights of Citizens, MIT Press (1973).

¹² Id. at 53.

such as to sell products or services to an individual, the Secretary's Advisory Committee recognized that an opt-out approach would be a practicable and appropriate form of consent.¹³

The Privacy Protection Study Commission's 1977 report also endorsed an opt-out approach for personal information which will not be used to make decisions affecting an individual's access to benefits or entitlements. In discussing the appropriate fair information practice approach to mailing lists and other databases used for marketing purposes, the Privacy Commission stated, "The negative check-off in some form is nonetheless the most convenient method for the individual to use, and is not without benefit to the organization that offers it."¹⁴

Almost 20 years later, in October of 1995, the Privacy Working Group's Report reached the very same conclusion. In the commentary to the Privacy Working Group's "fairness principle" (which reads, "Information users should not use personal information in ways that

¹³ Id. at 71-73. The Advisory Committee enunciated the following principles:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. Id. at 53-64.

¹⁴ Report of the Privacy Protection Study Commission, Personal Privacy in an Information Society, p.144 (1977).

are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use"), the report emphasizes that an information user seeking to use personal information in an incompatible manner must first notify the individual and, "obtain his or her explicit or implicit consent." The commentary goes on to discuss the appropriateness of opt-out versus opt-in, depending upon the use involved.

The nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing. In other cases, a notice offering the individual the ability to opt out of the use within a certain specified time may be adequate.¹⁵

A. Examples of Opt-Outs in Connection with Other Types of Personally Identifiable Information

1. Fair Credit Reporting Act, as Amended by the Consumer Credit Reporting Reform Act of 1996

Numerous statutes and regulations provide for an opt-out, even when the personal information at issue is arguably more sensitive than CPNI.

For example, the prescreening provisions of the Consumer Credit Reporting Reform Act of 1996 contain opt-out authorization.¹⁶ Consumer reporting agencies may provide consumer reports for credit and insurance prescreening purposes (marketing offers of credit or insurance), provided that the following opt-out options are offered:

¹⁵ Report of the Privacy Working Group, supra note 4, at 8.

¹⁶ The Consumer Credit Reporting Reform Act of 1996 was enacted as part of the Omnibus Consolidated Appropriations Act of 1997, Pub. L. No. 104-208.

- Written Notification: A signed notice of opt-out election form is distributed by the consumer reporting agency; or
- A Consumer Reporting Agency Notification System: A toll-free telephone number system; and an annual notification in a publication of general circulation that consumer reports may be used in this manner and the address and toll-free telephone number for consumers to use to select the opt-out option.¹⁷

CPNI (like consumer credit information when used for prescreening purposes) is used for marketing purposes, i.e., to acquaint consumers with the opportunity for new or enhanced telecommunications services. On the other hand, credit reporting information, in terms of its subject matter, is almost certainly more sensitive than CPNI information. Accordingly, the fact that the Congress in 1996 felt comfortable prescribing an opt-out procedure for this kind of use of credit reporting information provides support for applying an opt-out procedure to the use of CPNI.

2. Medical Directory Information

The Uniform Health Care Information Act ("Uniform Act"), adopted by the National Conference of Commissioners on Uniform State Laws and now enacted in several states, requires an opt-in for disclosures of health care information that is to be used for purposes of making decisions regarding benefits or entitlements but requires only an opt-out when the health care information at issue is less sensitive and where the information is unlikely to be used for purposes of determining benefits or entitlements. For example, Section 2-104(b)(1) of the Uniform Act provides that, "a health care provider may disclose health care information about a patient without the patient's authorization if the disclosure is directory information, unless the patient has instructed the health care provider not to make the disclosure."¹⁸

¹⁷ Consumer Credit Reporting Reform Act § 2404(a)(2) (to be codified at 15 U.S.C. § 1681b(e)).

¹⁸ "Directory information" is defined as "information disclosing the presence and the general health condition of a particular patient who is an in-patient in a health-care

Furthermore, the Uniform Act provides that, where the disclosure of personally identifiable health care information is to immediate family members or to any other individual with whom the patient is known to have a close personal relationship, or is to any health care provider who has previously provided health care to the patient, the disclosure can be made unless the patient has "opted-out" by "instruct[ing] the health care provider not to make the disclosure."¹⁹

3. Driver's Privacy Protection Act

In 1994, the Congress enacted the Driver's Privacy Protection Act in order to restrict the disclosure of personal information collected by state motor vehicle departments.²⁰ Under the Driver's Privacy Protection Act, state motor vehicle departments are permitted to disclose "personal information" (i.e., photograph, Social Security Number, driver identification number, name, address (excluding zip code), telephone number, and medical and disability information but not driving history), for certain categories of uses (i.e., government uses, motor vehicle safety uses); and for any other use, provided that the department has developed a system by which individuals are given adequate notification and an opportunity to opt-out.²¹

The Driver's Privacy Protection Act uses the opt-out approach, even though the information at issue is arguably more sensitive than CPNI, and even though the information can certainly be used for determining eligibility for benefits or entitlements. The factors that encouraged the Congress to rely on an opt-out included the history of motor vehicle

facility or who is currently receiving emergency health care in a health-care facility." § 1-102(2).

¹⁹ Section 2-104(a)(3) and (5).

²⁰ Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 18 U.S.C.A. § 2721 - § 2725.

²¹ Prior to the enactment of the Driver's Privacy Protection Act, the following seven states had enacted legislation permitting the disclosure of information held by motor vehicle departments subject to an opt-out: Delaware, Illinois, Maryland, New York, Oregon, Utah and Wisconsin.

information as public record information and the convenience of the opt-out for motor vehicle departments and the consumer.

4. State Opt-Out Statutes

In the last two years, numerous states have enacted information privacy legislation with opt-out provisions. Customarily, states have selected opt-out strategies for relatively non-sensitive types of personal information, such as "public records," or in circumstances where information is not being used to determine eligibility for benefits or entitlements.²²

5. Direct Marketing

The Direct Marketing Association ("DMA"), the national trade association for the direct marketing industry, encourages the direct marketing industry to adhere to the DMA's Fair Information Practice Guidelines ("Guidelines").²³ The DMA's fourth Guideline provides that, "An individual should have the ability to limit the disclosure of information about her or him that was obtained for one purpose from being disclosed for other unrelated purposes."²⁴ The

²² Vermont adopted legislation permitting telecommunications customers to opt-out of a database permitting the display of the customer's name in the state's enhanced emergency 911 system. Connecticut and Massachusetts both added opt-out provisions to privacy legislation relating to financial services information (Connecticut H. 6667, signed into law on June 6, 1995, and Massachusetts S. 79, signed into law on September 7, 1995). Alaska, Delaware, Iowa, Minnesota, New Hampshire, Tennessee and West Virginia have all enacted legislation in the last two years implementing the Driver's Privacy Protection Act and including opt-out provisions. Maine enacted direct marketing legislation with an opt-out provision (H. 100/LD 135, signed into law on June 27, 1995). Washington state enacted health and medical record legislation which includes an opt-out provision for certain "non-sensitive" types of medical record information (H. 1589, signed into law May 8, 1995).

²³ Direct Marketing Association, Inc., Fair Information Practices Manual, Chapter 2, p. 1.

²⁴ Id. at Ch. 2, p. 2.

system which the DMA supports for limiting such disclosures is to provide individuals with notice regarding the uses of customer lists and an opportunity to opt-out.²⁵

Under the DMA's Mail Preference Service ("MPS") and Telephone Preference Service ("TPS"), consumers may contact the DMA and request that their names be removed from the mailing lists of marketing companies which participate in the MPS.²⁶ Businesses subscribing to the MPS are notified periodically of the names of consumers who have exercised their opt-out option.²⁷

B. Model Notices and Opt-Out Language

Providing an effective notice at regular intervals and a convenient opportunity and method for consumers to communicate an opt-out is critical to the development of a meaningful opt-out system.

Literally thousands of companies have adopted notice and opt-out policies to apply to the disclosure of personal information -- particularly where the information does not involve highly sensitive categories of personal information and where the information is not being used or disclosed for purposes of making decisions regarding benefits or entitlements. We have collected a group of the best examples of opt-out notices in Appendix B.

²⁵ Id. at Ch. 2, pp. 2, 4.

²⁶ Id. at Ch. 2, pp. 7-8.

²⁷ Id. at Ch. 2, p. 11.

These notices share several common features:

- The opt-out notices describe the uses and disclosures in sufficient detail to be meaningful to the consumer and specifically identify information which is not disclosed and, therefore, not subject to the opt-out. Notices also concentrate on uses or disclosures that might not be anticipated by the consumer or do not seem to be compatible with the relationship or the purpose for which the consumer's information was first collected.
- The notices are relatively brief and, in general, do not exceed one page.
- The notices are in "plain English." The Federal Trade Commission and various consumer groups have done studies which establish the importance of expressing consumer notices in very simple, easy to understand language.
- The notices contain numerous headings and other visual cues.
- The notices explain how the opt-out works; how much time elapses between the time the opt-out designation is signed and returned to the recordkeeper and the time the opt-out goes into effect; the period of time for which the opt-out is effective and whether the opt-out must be renewed; and whether, and the extent to which, the opt-out applies to any new information about the consumer obtained by the third party recordkeeper after the date of the submission of the opt-out.
- Opt-out designations and notices which incorporate these kinds of characteristics have proven to be practicable and successful for third party recordkeepers and meaningful and effective for consumers.

IV. AFFILIATE SHARING

In recent years, the Congress and state legislatures have applied more flexible privacy rules when personal information is shared among corporate affiliates than when it is shared with third parties. This is especially apt to occur when the personal information at issue is not highly sensitive and/or the corporate affiliate is expected to use the information for a purpose compatible with the purpose for which the information was first collected or for a purpose, such as marketing, that does not involve a decision about access to entitlements or benefits. CPNI meets all of these criteria. The personal information comprising CPNI is not highly sensitive and a telecommunications carrier's affiliates will use CPNI for marketing purposes

-- not to make decisions about access to benefits or entitlements.

Public opinion research makes clear that the American public feels comfortable receiving marketing offers from corporate affiliates. A 1994 survey by Louis Harris and Associates conducted for MasterCard International and Visa U.S.A., with Alan Westin as academic consultant, found that 63 percent of the public feel that it is acceptable for "subsidiaries of the same corporate family" to share customer information "to make offers of services or products."²⁸

A variety of factors account for the public's comfort level with marketing offers from affiliated companies. The consumer, of course, already has a relationship with the company and has, therefore, already reposed a degree of trust in the company. Furthermore, consumers have expectations that companies share information among employees, contractors and agents in order to accomplish the mission for which the consumer's personal information was first collected. Where the sharing also includes another use which does not have a significant impact upon the consumer, such as a marketing use, it is apparent that disclosure and use by other corporate family members comes within the ambit of consumer expectations.

There are numerous examples of permissible sharing of personal information among affiliated parties. Under the Fair Credit Reporting Act, as amended, for example, reports pertaining to transactions or experiences of a consumer with a company which are then shared with an affiliate of that company ("persons affiliated by common ownership or common

²⁸ "Consumers and Credit Reporting 1994 Conducted for MasterCard International, Inc. and Visa U.S.A. Inc.," Louis Harris and Associates, Inc., pp. 11-12. More specifically, 71 percent of the public said that it was acceptable to offer a credit card to customers who have a mortgage with one of the credit card issuer's subsidiaries; 77 percent found it acceptable to offer a credit card to customers who have a checking account with the issuer's subsidiary; 70 percent found it acceptable to offer insurance to customers who have a loan with the insurance organization's subsidiary; and 71 percent said that it was acceptable to offer mutual funds to customers who have a checking account or loan with one of the subsidiaries. Id.

corporate control") do not fall within the definition of "credit report" and are, therefore, not subject to the Fair Credit Reporting Act.²⁹ Similarly, all other communications between a company and its affiliates are not considered "credit reports" as long as the consumer is provided with a notice that the information may be communicated between the company and its affiliates and the consumer has an opportunity to "direct that such information not be communicated among such persons."³⁰

As another example, numerous health and medical record privacy bills and statutes permit the sharing of health information with agents and contractors, as well as other health care providers who have previously provided care to the patient (the NCCUSL Uniform Law includes this kind of provision) on the theory that these are affiliated persons who not only have a need for access to the information but, perhaps more importantly, present less of a privacy threat with respect to the use of the information.

Even various information privilege laws recognize the concept of affiliated parties. Under both the lawyer-client and the doctor-patient privileges, for example, disclosures to affiliated parties sharing a common interest do not necessarily forfeit the privilege.³¹ The courts and the common law have come to recognize that these disclosures are often necessary and useful to effectuate the purpose for which the privilege exists and are not inimicable to confidentiality and the prohibitions against third party disclosure on which all information privileges rest.

²⁹ Consumer Credit Reporting Reform Act, § 2402(e), § 2419(2). See, § 2411(e) ("Duties of Person Taking Certain Actions Based on Information Provided by Affiliate") (amending 15 U.S.C. § 1681m(c)). See, also, Andrew Taylor, Bank Regulations Eased, Congressional Quarterly, Dec. 7, 1996, at 3358.

³⁰ Consumer Credit Reporting Reform Act, § 2402(e).

³¹ See, United States v. McPartlin, 545 F.2d 1321, 1335-37 (7th Cir.), cert. denied, 444 U.S. 833 (1979).

V. CONCLUSION

We appreciate this opportunity, on behalf of the Pacific Telesis Group, to present information regarding the "sensitivity" of CPNI; the appropriateness of an opt-out procedure for CPNI; and the relative absence of a privacy threat when CPNI is disclosed among affiliated parties.

Respectfully submitted,



Alan F. Westin *by RRB*



Robert R. Belair

Privacy & Legislative Associates, Inc.
1150 Connecticut Avenue, N.W., Suite 700
Washington, DC 20036
(202) 296-2862

On behalf of Pacific Telesis Group

APPENDIX A

Privacy & Legislative Associates, formed in 1993, specializes exclusively in privacy matters. The two founders and principals, Alan F. Westin and Robert R. Belair, have a combined 70 years of experience as lawyers and political scientists in the privacy arena.

Dr. Westin is widely regarded as the nation's leading privacy expert, having written dozens of books and monographs on the subject including *Privacy and Freedom* and *Databanks in a Free Society*, two seminal works in the field. He has also pioneered in public opinion and survey research on privacy and has served as privacy advisor to many of the nation's largest and best known corporations.

Robert Belair is a Washington lawyer specializing in privacy matters. Mr. Belair has served as an attorney at the Federal Trade Commission, handling, among other things, Fair Credit Reporting Act matters and as Deputy Counsel of the White House Committee on the Right of Privacy. Mr. Belair has served as General Counsel of the National Commission on the Confidentiality of Health Records and as a privacy lawyer and consultant for numerous government agencies and commissions including the National Science Foundation, the National Paperwork Commission and the National Academy of Sciences.

APPENDIX B

MODEL NOTICES AND OPT-OUT LANGUAGE

Many companies that collect information about customers, particularly companies collecting non-sensitive personal information, have developed and currently implement methods by which they notify customers of the companies' policies regarding the disclosure of personal information and customers' options to opt-out of such disclosures. The most effective notices and opt-out provisions provide adequate notice regarding possible uses or disclosures of the information and the opt-out option and are clear, concise and written in "plain English." The following are examples of notice and opt-out provisions that meet these criteria.

An Important Notice Concerning Cardmember Privacy, Mailing, and Telemarketing Options

At American Express, we want you to understand all that the Card affords you, including the offers you receive through the mail and by telephone.

These offers come directly from us, from our affiliates, from establishments that accept the Card, or from other well-established companies. Each offer is carefully developed to ensure that it meets our standards. Additionally, we try to make sure that these offers reach only those Cardmembers most likely to take advantage of them.

To do this, we develop lists for use by us and our affiliates based on information you provided on your initial application and in surveys, information derived from how you use the Card that may indicate purchasing preferences and lifestyle, as well as information available from external sources including consumer reports.

We may also use that information, along with non-credit information from external sources, to develop lists which are used by the companies with whom we work.

These lists are developed under strict conditions designed to safeguard the privacy of Cardmember information.

Notice to New Cardmembers: Your name and address will be suppressed from marketing mailing lists used by non-American Express companies for four weeks after you have been accepted for Cardmembership to give you an opportunity to elect not to receive marketing mailings in accordance with this notice.

Many Cardmembers tell us they appreciate these offers, as well as information on Cardmember benefits. However, if you no longer wish to receive these offers and information about benefits, please select one or more of the following options:

- Please exclude me from American Express mailings, including new benefits and American Express Merchandise Services catalogs.
- Please exclude me from mailings by other companies, including offers in cooperation with American Express provided by establishments that accept the Card.
- Please exclude me from lists used for telemarketing.

If you have previously informed us of your preferences, you do not need to complete this form unless you have new accounts to add, or wish to change your selections.

Please enter all of your American Express and Optima® Card account numbers for which you would like the options to apply.

- Check here if you also wish these selections to apply to Additional Cardmembers on your account(s).

Please note:

- 8 to 10 weeks are generally required for your request to become effective.
- So that you receive important information about the Card, we may continue to enclose notices in your monthly account statement, and on a very limited basis, we may send you other notices from American Express.

¹ Handbook of Company Privacy Codes (Vol. 3, 1996) (compiled by *Privacy & American Business*), 13-14.

HARRON CABLEVISION²

SUBSCRIBER PRIVACY NOTICE

Section 631 of the Cable Communications Policy Act of 1984, as amended by the Cable Television Consumer Protection and Competition Act of 1992 ("Cable Act") requires us to inform you of the following information annually:

1. So that we may continue to provide reliable, high quality service to you, we keep regular business records that contain your name, address, and other personally identifiable information. Such records include billing, payment and deposit records, records indicating the number of television sets you have connected to cable, and the service options you have chosen. We use this information to make sure that you are being properly billed for the service you receive. We also use this information to sell, maintain, disconnect, and reconnect services, for service calls, customer surveys, bill collections, in-house telemarketing, our own tax and accounting records, statistics, demographic studies, and the detection and prosecution of theft of services. We take reasonable precautions to prevent unauthorized access to this information.

2. We consider information we keep to be confidential. We may collect personally identifiable information from you and may disclose it to a third party if (a) you consent in advance in writing or electronically; (b) disclosure is necessary to render cable service and other services we provide to you and related business activities; or (c) disclosure is required under court order, and you are notified of such order. Disclosure "necessary to render cable services" includes release of personally identifiable information to employees, contractors, and other agents of the company to install, market, provide and audit cable service; to collection agencies if necessary to collect past due bills; to program suppliers (or their agents) to send program guides and for auditing purposes; to our attorneys and accountants if required for the proper functioning of our business; to third party billing systems to prepare and send your bills; and to our attorneys and law enforcement agencies if necessary for the detection and prosecution of theft of services.

3. Unless you object, from time to time, we may also disclose your name and address for cable-related mailing lists and other purposes. This information may also be used for surveys and various marketing mailings. We will not disclose the extent of your viewing or use of a particular service or the nature of any transaction you may make over the cable system, but we may disclose that you are among those who subscribe to a particular service. If you wish to remove your name from such lists or limit the use of your name at any time, please contact us in writing. Your written notification should **NOT** be sent with your payment, it should be mailed to your local Harron Cable TV office. The local office address appears on the top left corner of your bill.

Please note, however, Harron does not release the names and addresses of its customers to any third party except as it relates to providing legitimate cable-related services to our customers.

4. We may also electronically test the system from time to time to determine whether you are being properly billed for the cable services you are receiving.

5. We will maintain information about you for as long as we provide service to you, and for a longer time if necessary for related business activities. Ordinarily, for tax reasons, we would keep records for six (6) years. When information is no longer necessary for our purposes, we will destroy the information unless there is a legitimate request or order to inspect the information still outstanding.

6. You have the right to inspect our records that contain information about you, correct any error in our information, and enforce your rights under federal law. Included among your federal rights is the right to participate in a proceeding in which the government seeks to obtain your personally identifiable information from the company. If you wish to inspect the records at our system office pertaining to you or review your statutory rights, please contact us to set up an appointment during regular business hours.

7. Federal law limits our collection and disclosure of personally identifiable information, except as described above. An aggrieved party may bring a private action to enforce his/her federal rights, including recovery of statutory damages and costs.

8. If you have previously notified us, **in writing**, to remove your name from any mailing list, it is **NOT** necessary to notify us again.

² Handbook of Company Privacy Codes (Vol. 2, 1995) (compiled by *Privacy & American Business*), 10.

PRIVACY RIGHTS³

IMPORTANT SUBSCRIBER PRIVACY NOTICE

Cable television subscribers are entitled to certain privacy rights under the Cable Communications Policy Act of 1984. The act restricts the ways in which we may collect, retain and disclose personally identifiable subscriber information, and requires us to inform you of your rights and remedies.

We maintain records containing your name, address, telephone number, and information concerning service packages and equipment, and service complaints and repairs. Our records also contain information on billing and payment including (for new subscribers after 9-1-91) credit information as well as credit card information for pay-per-view events. We use this information to provide the services you order and for billing, tax, accounting, marketing and research functions.

We will not disclose personally identifiable subscriber information to any third party without a subscriber's prior consent, except when disclosure is necessary to provide our services or to conduct our business. We may provide information to outside contractors and engineers to perform installation, maintenance, or repair functions; to computer services and accountants for billing, collection, and financial purposes; to program suppliers for audit purposes; and to distributors to provide program guides. In addition, law enforcement authorities may obtain personally identifiable subscriber information from our records upon court order. You must be afforded the opportunity to appear in court and contest the government's claim. We're required to notify you if a court order is entered requiring us to make disclosure.

We are sometimes requested by outside parties such as charities, independent contractors that conduct advertising and program research, and direct order retailers to supply them with subscribers' names, addresses and services subscribed to. If you don't want to have this information disclosed to these entities, complete the form below and return it to us. Under no circumstances will we provide any information which discloses to them the extent to which you view or use any of our services or the nature of transactions you make through our cable system.

Personally identifiable information about you will be collected and retained for so long as you remain a subscriber to our system. Thereafter, we will retain such information only for so long as is necessary to complete billing and accounting functions and as otherwise required by law.

No personally identifiable subscriber information will be disclosed to third parties after a subscriber ceases to be a subscriber.

You have the right to examine all personally identifiable information about you which we are maintaining at any time during our normal business hours at our offices at 14650 Old Lee Road, Chantilly, Virginia. You may bring to our attention any errors which you believe to exist in such information.

Cable subscribers whose privacy rights are violated under the act may, in addition to any other remedies, bring a civil suit in federal court. The court may award actual or liquidated damages, punitive damages, attorney's fees and litigation costs incurred by the subscriber.

SUBSCRIBER PRIVACY - REPLY FORM

If you don't want to have your name and address disclosed to the organizations described in the enclosed Subscriber Privacy Notice, complete this form and return it to:

**Media General Cable
Attn: Communications Department
14650 Old Lee Road, Chantilly, VA 22021**

Signature: _____
Print Your Name: _____
Address: _____
Account Number: _____ Date: _____

Personal Identification Numbers (PIN codes) are available upon request to ensure privacy regarding your cable service account. For information please call 378-8422.

³ Handbook of Company Privacy Codes (1994) (compiled by *Privacy & American Business*), 9.