No. 99-1427

IN THE
SUPREME COURT OF THE UNITED STATES
OCTOBER TERM, 1999

COMPETITION POLICY INSTITUTE,

Petitioner,

v.

U S WEST, INC.,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUIT

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER, 14 CONSUMER ORGANIZATIONS, AND 19 LAW PROFESSORS AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

Of Counsel:

MARC ROTENBERG
DAVID L. SOBEL
ELECTRONIC PRIVACY
INFORMATION CENTER
1783 Connecticut Ave., N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

JONATHAN D. BLAKE
Counsel of Record
KURT A. WIMMER
AMY L. LEVINE
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
Washington, DC 20004
(202) 662-6000
Counsel for Electronic Privacy Information Center

May 1, 2000

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

LEGISLATIVE MATERIALS

ADMINISTRATIVE MATERIALS

OTHER

INTEREST OF THE AMICI CURIAE

All *amici curiae* represented in this brief have acquired considerable practical experience addressing privacy rights.[1] The ruling of the court of appeals at issue here threatens the personal privacy rights that these *amici* strive to protect. It also conflicts with this Court's decision in *Reno v. Condon*, holding that Congress has the constitutional authority to decide that an organization may be barred from disclosing certain information about a person unless it obtains that individual's express consent.

Amicus the Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

Amicus AARP is a non-profit organization with more than 33 million members age 50 and older. AARP is greatly concerned about ensuring strong consumer protections in the marketplace and thus supports laws and public policies to protect consumers' privacy rights.

Amicus Center for Center for Media Education ("CME") (Jeff Chester, Director) is a national non-profit organization that works to ensure electronic commerce consumer protections for children and families. In 1998,

---

[1] The parties have consented to the filing of this brief. Their letters are on file with the Clerk of the Court. Pursuant to Rule 37.6, *amici* state that no counsel for any party has authored this brief in whole or in part, and no person or entity other than *amici* made a financial contribution to the preparation or submission of this brief.

CME's effort led to the Congressional passage of the Children's Online Privacy Protection Act.

Amicus Colorado PIRG ("CoPIRG") is a non-profit, non-partisan consumer advocacy organization with 42,500 members around the state of Colorado. We support efforts, both statewide and nationally, to protect the privacy of our members and of consumers generally.

Amicus Computer Professionals for Social Responsibility ("CPSR") (Coralee Whitcomb, President) is a public interest alliance of computer scientists and others concerned about the impact of computer technology on society.

Amicus Consumer Action (Ken McEldowney, Executive Director) is an educational and advocacy organization that works on a wide range of consumer and privacy issues impacting low income and limited English speaking consumers.

Amicus Consumer Federation of America ("CFA"), established in 1968, represents more than 260 organizations from throughout the nation with a combined membership exceeding 50 million people and works to advance pro-consumer policy on a variety of issues before Congress, the White House, federal and state regulatory agencies, and the courts.

Amicus International Communications Association ("ICA") (Brian R. Moir, Counsel) is the largest association of telecom end users in the United States. Its more than 500 members are all users (not vendors) of telecommunications services, and collectively they spend in excess of $32 billion per year on telecom/IS expenses.

Amicus Junkbusters (Jason Catlett, President) operates a popular web site on consumer privacy. Junkbusters President Jason Catlett has a Ph.D. in Computer Science; prior to founding Junkbusters he worked on data mining of call detail records for several years at AT&T Bell Laboratories.

Amicus Media Access Project (Andrew Jay Schwartzman, President and CEO) is a non-profit public interest telecommunications law firm founded in 1972. It represents the public's First Amendment right to have affordable access to a vibrant marketplace of issues and ideas via telecommunications services and the electronic mass media.

Amicus New Mexico PIRG ("NMPIRG") is a non-profit, nonpartisan, consumer advocacy organization with 4,000 members around the state of New Mexico. NMPIRG has supported efforts, both statewide and nationally, to protect the privacy of its members and of consumers generally.

Amicus Privacy International ("PI") (Simon Davies, Director General) is an international human rights organization, based in London, England with an office in Washington, DC and members in over 40 countries. PI advocates for legal and technical measures to protect the right of privacy.

Amicus Privacy Rights Clearinghouse ("PRC") (Beth Givens, President) is a non-profit consumer information and advocacy program established in 1992, based in San Diego, California. It advocates for consumers' privacy rights in legislative and regulatory proceedings at the state and federal levels.

Amicus Private Citizen, Inc. ("PCI") (Robert Bulmash, President and Founder) was formed in 1988 to protect residents and businesses from the privacy-abusing practices of the direct marketing industry.

Amicus U.S. Public Interest Research Group ("U.S. PIRG") is a non-profit, non-partisan consumer, environmental, and good government advocacy organization that serves as the national lobbying office for state PIRGs. U.S. PIRG and the state PIRGs advocate strong privacy laws on behalf of both their more than 500,000 dues-paying citizen members nationwide and consumers generally.

Pam Samuelson, Professor of Law, Co-Director of the Berkeley Center for Law & Technology Boalt Hall, University of California at Berkeley.

Ann Bartow, Visiting Assistant Professor of Law, University of Dayton School of Law

Thomas F. Blackwell, Assistant Professor of Law, Appalachian School of Law

Julie E. Cohen, Associate Professor of Law, Georgetown University Law Center.

Peter L. Fitzgerald, Associate Professor, Stetson University College of Law.

Susan Freiwald, Associate Professor of Law, University of San Francisco School of Law

A. Michael Froomkin, Professor of Law, U. Miami School of Law.

Shubha Ghosh, Associate Prof. of Law, GSU College of Law

Evan Hendricks, Publisher of The Privacy Times

Jerry Kang, Professor of Law, UCLA School of Law

Michael Madison, Professor of Law, University of Pittsburgh School of Law

Eugene R. Quinn, Jr., Assistant Professor of Law, Barry University of Orlando School of Law

Joel R. Reidenberg, Professor of Law and Director of the Graduate Program Fordham University School of Law

Michael Rustad, Professor of Law & Director of the High Technology Law Program, Suffolk University Law School.

Paul M. Schwartz, Professor of Law, Brooklyn Law School.

Robert Ellis Smith, Publisher of The Privacy Journal; author, The Law of Privacy Explained.

David E. Sorkin, Assistant Professor of Law and Associate Director, Center for Information Technology & Privacy Law, The John Marshall Law School

Frank Tuerkheimer, Professor of Law, University of Wisconsin, School of Law.

Jonathan Weinberg, Professor of Law, Wayne State University.

SUMMARY OF THE ARGUMENT

I. The decision of the court of appeals undermines basic tenets of an individual's right to privacy under federal law. Citizens have a legitimate expectation of privacy with respect to sensitive personal information such as who they call on a telephone, and a carrier's right to communicate information about products and services does not include the right to build detailed profiles based on personal information obtained through private telephone calls.

II. The FCC's CPNI Order is analogous to numerous other federal laws and regulations implemented to protect citizens' privacy and does not implicate any First Amendment concerns.

III. The opt-in approach adopted by the FCC's CPNI Order reflects Congress's express intent in enacting Section 702 of the Telecommunications Act to protect the privacy of telephone customers. This Court explicitly endorsed such an opt-in approach in the analogous context of protecting information an individual discloses to her state DMV in *Reno v. Condon*, decided earlier this Term.

ARGUMENT

I. THE DECISION OF THE TENTH CIRCUIT PANEL JEOPARDIZES AN INDIVIDUAL'S RIGHT TO PRIVACY.

American jurisprudence recognizes a fundamental right to privacy in personal communications, and both the courts and Congress have recognized the paramount interest a citizen has in protecting her privacy. *See, e.g.*, *Edenfield v. Fane*, 507 U.S. 761, 769 (1993) ("[T]he protection of potential clients' privacy is a substantial state interest."); *Sheets v. Salt Lake County*, 45 F.3d 1383 (10th Cir. 1995).

Most recently, this Court held earlier this year in *Reno v. Condon*, ____ U.S. _____, 120 S. Ct. 666 (2000), that Congress can restrict the ability of state departments of motor vehicles ("DMV"s) to disclose personal information about a driver without that driver's express consent. *See id.* at 668-69. Because the decision of the court of appeals in this case fails to recognize an individual's paramount right to keep private her most personal information, this Court should grant certiorari and overturn the court of appeals' ruling or remand it for reconsideration in light of this Court's holding in *Reno v. Condon*.

A. Individuals Have A Significant Interest In Controlling Distribution Of Their Personal Information And In Preventing Others From Profiting By Its Use.

In *Lanphere & Urbaniak v. Colorado*, 21 F.3d 1508 (10th Cir. 1994), the court of appeals recognized that an invasion of privacy is most pernicious when "it is by those whose purpose it is to use the information for pecuniary gain." *Id.* at 1511, 1514. This is exactly the purpose for which Respondent would like to use CPNI -- to target consumers it believes might be interested in purchasing more of its services. The fact that some CPNI, such as a consumer's name and address, may be publicly available is irrelevant, because "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form." *Department of Defense v. Federal Labor Relations Auth.*, 510 U.S. 487, 500-02 (1994) (finding that unions could not use FOIA to obtain the home addresses of federal employees represented by unions).

In addition, the protections afforded by the FCC's regulation go well beyond concerns with the use or

disclosure of publicly available information. The regulation and the underlying statute also protect even more sensitive data about telephone numbers the customer called or from which the customer received a call and the length of the call. As Justice Stewart wrote:

> Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

It is notable that Congress recognized the importance of a citizen's privacy interest by enacting other statutes preventing disclosure of precisely the same information to the public at large. For example, Congress has enacted an elaborate statutory scheme to protect the privacy of telephone communications, *see* 18 U.S.C. §§ 2510-2522 (1994 & Supp. IV 1998), and specifically prohibited the use of pen registers without a court order. *See* 18 U.S.C. § 3121 (1994). Thus, the Congress has determined that people have a legitimate expectation of privacy with respect to the phone numbers they dial and has decided that this information is so sensitive that it has developed an entire statutory scheme governing law enforcement's ability to collect such data. Similar rules have been established to protect the privacy of cable subscriber records, *see* 47 U.S.C. § 551 (1994), video rental

records, *see* 18 U.S.C. § 2710 (1994), credit reports, *see* Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994), and medical records, *see* 42 U.S.C. § 290dd-2(a)(1994). *See generally* Marc Rotenberg, *The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Developments* 1-173 (1999). The panel's decision fails to accord the proper degree of weight to this valid expectation of privacy.

In contrast to the court of appeals' disregard for personal privacy, this Court earlier this term in *Reno v. Condon* recognized that Congress has the authority to protect an individual's personal information when it upheld the constitutionality of the Driver's Privacy Protection Act, 18 U.S.C. § 2721 (1994 & Supp. IV 1998), which prohibits state DMVs from disclosing personal information about its drivers without their express consent. *See infra* Section III.C.

Further, the FCC's CPNI rule not only protects the privacy interests of telephone customers, but also preserves important values recognized in the First Amendment context, which is the right of telephone customers to decide, freely and without unnecessary burden, when they wish to disclose personal information to others. *See generally Buckley v. American Constitutional Law Found., Inc.*, 525 U.S. 182 (1999); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995); *Talley v. California*, 362 U.S. 60 (1960). The ability of individuals to keep private the records of their personal communications also implicates the constitutional interest in not chilling communications between free individuals through the fear of private surveillance. *See NAACP v. Alabama*, 357 U.S. 449, 462 (1958); *see also Smith v. Maryland*, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting).

B. The FCC's CPNI Order Does Not Unlawfully Restrict Respondent's Right To Communicate With Its Customers.

In its opinion, the court of appeals relied on cases including *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748 (1976), *Martin v. City of Struthers*, 319 U.S. 141 (1943), and *Florida Bar v. Went For It, Inc.*, 515 U.S. 618 (1995), to support the proposition that the government cannot restrict the speech of either a speaker or his audience. However, each of these cases turns on the method of communication and not the use of personal information acquired from business customers. The FCC's Order does not prevent Respondent from advertising its services to its customers per *Virginia Pharmacy* or pamphleteering per *Struthers* or using direct mail per *Florida Bar*. But none of these cases involves a service provider using confidential information to target a particular audience. In *Shapero v. Kentucky Bar Ass'n*, 486 U.S. 466 (1988), for example, this Court upheld certain targeted solicitations by lawyers; however, the attorneys were able to obtain information about their intended audience from public records.

What the FCC's CPNI Order prohibits is Respondent's nonconsensual use of confidential consumer information, generated by customers in the course of their private activities, to advertise products and services. The effect of the decision of the court of appeals is to require essentially captive subscribers to forfeit truly personal information to whatever purpose a telecommunications provider thinks may provide a commercial benefit. This is an exploitative business practice clothed in the garb of the commercial speech doctrine.

II. THE FCC'S CPNI ORDER NEED NOT IMPLICATE FIRST AMENDMENT CONCERNS.

Many state and federal laws limit the disclosure of personal information by private entities without implicating the First Amendment. For example, the Fair Credit Reporting Act provides that a credit agency can only release a consumer's credit report under certain conditions and criminalizes unauthorized disclosures by employees of the consumer reporting agency. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681r (Supp. III 1997); *see also* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994) (prohibiting disclosure of a consumer's video rental records).

In addition, this Court has held unequivocally that a commercial entity that is not a news publication cannot claim full First Amendment protection for the information it includes in a credit report. *See Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762 (1985). Such speech receives lesser protection because it is "solely in the individual interest of the speaker and its specific business audience." *Id.* As a commercial entity that desires to use private information it has obtained from its customers for its own pecuniary gain, U S West is entitled to, at most, limited First Amendment protection.

If this Court is prepared to allow a commercial entity to claim a First Amendment interest in the commercial use of private information obtained from its customers, it will call into question virtually every law in the United States that seeks to protect the privacy of consumers. As telephone companies, Internet service providers, and other communications firms acquire ever more detailed information from customers in the course of offering routine communication services, the ruling of the court of appeals could effectively prevent the adoption of legislative

safeguards that would preserve the reasonable expectation of privacy in private communications and personal activities that telephone customers currently enjoy.

III. THE FCC PROPERLY INTERPRETED THE INTENT OF THE CONGRESS BY CHOOSING THE MOST EFFECTIVE MEANS FOR PROTECTING THE PRIVACY INTERESTS OF CONSUMERS.

When Congress enacted section 702 of the Telecommunications Act of 1996, its primary concern was protecting the privacy interests of consumers. Congress did not intend to impede the carrier's ability to communicate with its current or potential customers but rather to insist that confidential information remain protected.

A. **Congressional Intent Makes Clear That § 222 Applies To The Rights Of Customers, Not Carriers.**

47 U.S.C. § 222(c)(1) requires a telecommunications carrier to obtain a customer's approval before it can use, disclose, or allow access to that customer's CPNI. *See* Telecommunications Act of 1996 § 702(c)(1), 47 U.S.C. § 222(c)(1) (Supp. III 1997). In its report on the legislation that was eventually enacted as the Telecommunications Act of 1996, the House Commerce Committee explained that the purpose of the protections contained in this section is to balance "the need for customers to be sure that personal information that carriers may collect is not misused" against the customer's interest in ensuring "that when they are dealing with their carrier concerning their telecommunications services, the carrier's employees will have available all relevant information about their service." H.R. Rep. No. 104-204, pt. 1, at 90 (1995).

Respondent's argument that it has a First Amendment right to disclose CPNI is compromised by the fact that customers provide this information with the reasonable expectation that it will be kept confidential and that customers have no choice regarding their carrier's collection of this data. This Court, as well as the court of appeals, has held that if the state possesses extremely personal information about an individual, that individual has a legitimate expectation of privacy with respect to that material, and the government can only disclose it in certain narrow circumstances. *See Nilson v. Layton City*, 45 F.3d 369, 372 (10th Cir. 1995); *see also Whalen v. Roe*, 429 U.S. 589, 599 & n.24 (1977). To be able to disclose such information, (1) the party asserting the right must have a legitimate expectation of privacy, (2) disclosure must serve a compelling state interest, and (3) disclosure must be made in the least intrusive manner. *See Flanagan v. Munger*, 890 F.2d 1557, 1570 (10th Cir. 1989); *Denver Policemen's Protective Ass'n v. Lichtenstein*, 660 F.2d 432, 435 (10th Cir. 1981).

Although a telecommunications carrier is not the state, applying the *Denver Policemen's* test is instructive. A customer has a legitimate expectation of privacy with respect to CPNI because this data is not publicly accessible. In addition, there is no compelling state interest in promoting CPNI disclosure that could not be served in a less intrusive manner through the opt-in, rather than the opt-out, approach. In either case, the carrier can only reveal CPNI with the customer's consent, and the opt-in approach is least intrusive to the consumer.

B. Congressional Intent Makes Clear That "Approval of a Customer" Requires An Opt-In Approach.

Section 222(c)(1)'s requirement that a carrier seek a customer's "approval" before disclosing her CPNI demonstrates that the FCC's adoption of an opt-in approach is in line with congressional intent. When the FCC contemplated its order, it primarily considered two options: opt-in and opt-out. Under an opt-in approach, consumers must give the carrier express approval before the company can divulge their CPNI, which, as the FCC explained, "will minimize any unwanted or unknowing disclosure" of the information. CPNI Order at 20,329. With an opt-out approach, by contrast, customers would receive a notice to sign and return to prevent the carrier from disclosing their CPNI. As the FCC explained, the danger of the opt-out approach is that "because customers may not read their CPNI notices, there is no assurance that any implied consent would be truly informed." *Id.*

Black's Law Dictionary defines "approval" as "[t]he act of confirming, ratifying, assenting, sanctioning, or consenting to some act or thing done by another. 'Approval' implies knowledge and exercise of discretion after knowledge." Black's Law Dictionary 102 (6th ed. 1990); *see also* Webster's II New College Dictionary 56 (1995) (defining "approve" as "[t]o confirm or agree to officially"). The opt-out approach fails to satisfy this definition of "approval" because the customer is not confirming or ratifying anything. Under the opt-out approach, consumers may not possess the knowledge that they must affirmatively act to prevent carrier distribution of their CPNI. If they do not have this knowledge, then they cannot exercise discretion regarding it.

The real question before this Court is what the default position should be for consumers who are unaware of their telecommunications carrier's CPNI policies and whether those customers' privacy rights should be protected. With opt-in, the default is that the customer's personal information cannot be disclosed. Under opt-out, the default is that the carrier is free to disclose this sensitive information.[2] A customer has a reasonable expectation that his personal information will be kept private. This expectation is upset under the opt-out approach, pursuant to which the carrier can sell this data without consulting with the customer. Congress's use of the word "approval" indicates that the default position should favor the uninformed consumer; i.e., if a customer does not sanction the disclosure of his CPNI, then his CPNI should remain confidential. Because "approval" requires an affirmative action by an informed consumer, only the opt-in approach endorsed by the FCC in its CPNI Order satisfies congressional intent. It is the most reasonable fit between Congress's ends and the means chosen to reach those ends.

---

[2] Although under the opt-out approach the consumer would receive some type of notice or form from his telecommunications carrier explaining what CPNI is and how the carrier would like to use it and instructing the individual to sign and return the form to preclude the carrier's use of this data, the fact is that many consumers will fail to read such an instrument or will misplace it or forget to return it to the company. Thus, there is the danger that a number of customers who do not want their CPNI revealed will fail to contact their carrier to opt-out because they are either forgetful, uncertain, or uninformed.

C. Congress's Actions In Enacting CPNI Protection Are Directly Analogous To Its Enactment Of The DPPA.

In *Reno v. Condon*, ____ U.S. ____, 120 S. Ct. 666 (2000), decided earlier this year, this Court upheld the Driver's Privacy Protection Act of 1994 ("DPPA"), 18 U.S.C. § 2721 (1994 & Supp. IV 1998), which prohibits states from disclosing personal information contained in the records of their respective Departments of Motor Vehicles ("DMV") without a driver's express consent. Chief Justice Rehnquist, writing for a unanimous bench, agreed "that the personal, identifying information that the DPPA regulates is a 'thin[g] in interstate commerce,' and that the sale or release of that information in interstate commerce is therefore a proper subject of congressional regulation." *Id.* at 671. CPNI is also personal, identifying information that is a proper subject of congressional regulation as a thing in interstate commerce. In fact, CPNI is arguably even more personal than the information in DMV records because while DMV records are typically updated only once every few years, each time a citizen renews her driver's license or registers a new vehicle, CPNI is updated constantly, every time an individual makes or receives a phone call.

Even more compelling is the fact that this Court in *Condon* explicitly upheld a regulation that utilizes an opt-in approach. When this Court granted certiorari in *Condon*, the DPPA employed an opt-out approach, pursuant to which the DMV could disclose the driver's information unless the driver objected. *See id.* at 669. By the time the case was argued, Congress had amended the DPPA to require an opt-in approach, so that "States may not imply consent from a driver's failure to take advantage of a state-afforded opportunity to block disclosure, but must rather obtain a driver's affirmative consent to disclose the driver's personal information for use in surveys, marketing, solicitations, and

other restricted purposes." *Id.* What is most important is that this Court did not find an opt-in approach overly restrictive or, as the court of appeals held with respect to CPNI, that the DPPA had to employ the least restrictive means of achieving its end.

CONCLUSION

For the reasons set forth above, *amici* EPIC and the AARP respectfully urge the Court to grant certiorari and reverse the decision of the court of appeals, or alternatively to remand in light of *Reno v. Condon*.

Respectfully submitted,

Of Counsel:

MARC ROTENBERG
DAVID L. SOBEL
ELECTRONIC PRIVACY
INFORMATION CENTER
1783 Connecticut Ave., N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

JONATHAN D. BLAKE
Counsel of Record
KURT A. WIMMER
AMY L. LEVINE
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
Washington, DC 20004
(202) 662-6000
Counsel for Electronic Privacy Information Center

DATED: MAY 1, 2000