BLOCKING PREEMPTION: CONVERGENCE, PRIVACY, AND THE FCC'S MISGUIDED REGULATION OF CALLER ID

INTRODUCTION 408
I. THE VALUE AND DANGERS OF INFORMATION 411
II. CALLER ID 414
A. *The Business Community's Best Friend* 415
B. *Blocking Measures* 417
III. FCC RULING 418
A. *Reasons for the FCC Ruling* 420
B. *Problems with the FCC Ruling* 421
IV. A PROPOSAL TO PRESERVE THE PRIVACY INTERESTS OF CALLERS 426
A. *Consumer Education* 428
B. *Per-Call Blocking as a Minimum Standard* 429
V. THE FCC'S PREEMPTION OF STATE LAW 430
A. *Congress's Power to Preempt State Law* 430
B. *The Validity of Agency Rules that Preempt State Law* ... 431
C. *Case Law Regarding the FCC's Statutory Authority* 432
D. *The FCC's Authority to Preempt State Regulation of Caller ID* 433
E. *Convergence and Existing Privacy Protections* 434
1. The Cable Television Consumer Protection Act 435
2. The Video Privacy Protection Act of 1988 437
3. Telephone Consumer Privacy Protection Act of 1993 438
4. Study Commissions on Privacy Issues 440
a. Committee on Automated Personal Data Systems 440
b. Nixon's Domestic Council Committee on the Right to Privacy 441
c. Privacy Protection Study Commission 441
d. The National Telecommunications and Information Administration's Recognition of Increased Privacy Requirements in the Age of the Information Superhighway 443
F. *Implications of Existing Statutes and Previous Study Commissions* 444
CONCLUSION 445

> The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[1]
>
> *Justice William Brennan, 1976*

INTRODUCTION

Advances in technology have led us towards an information-dependent global economy that threatens to make public the details of our private lives.[2] Soon, Americans will be able to access numerous commercial, scientific, and business databases, along with services such as participatory television, banking, home shopping (with price comparisons of neighborhood stores), and remote medical testing.[3] Despite the convenience of such dynamic technological advances,[4] the increased number of electronic transactions, accelerated collection of personal information, and advances toward interconnectivity of telecommunications networks and information service providers spawn intense public concern about personal privacy.[5] Inevitably, the proliferation of multimedia services will create "the electronic equivalent of a paper trail" that will

---

[1] Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring).

[2] Fred H. Cate, *The Future of Communications Policymaking*, 3 WM. & MARY BILL R.J. 1 (1994).

[3] In a recent inquiry, the Department of Commerce envisioned the information superhighway as a phenomenon that

> could ultimately provide access to interactive multimedia, integrated digital streams of video, audio, text, and graphics that will allow an instantaneous dialogue between the user and the system for the transmittal of information. Interactive multimedia encompasses such services as video on demand, participatory television, electronic publishing, interactive video games, teleshopping, telebanking, videoconferencing, remote medical testing and evaluation, and distance learning. For example, using devices with the attributes of a telephone, a television, a camcorder, and a personal computer, students ultimately may be able to browse through the collections of any library in the country and collaborate on research projects with others hundreds of miles away, individuals may be able to experience special family events like a christening or wedding even though they cannot attend in person, and citizens may be able to participate in electronic town meetings. In addition, small businesses as well as large may take advantage of the latest in computer technology to design products and provide useful services . . . .

Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842, 6843-44 (1994) (footnote omitted).

[4] "We look forward to the dissemination of high-definition television, virtual reality, and artificial intelligence. These and other 'back-to-the-future' wonders will continue to transform our world in the years and decades ahead." Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH. 1, 1 (1992).

[5] 59 Fed. Reg. 6842; *see Whalen*, 429 U.S. at 605 (stating that "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information . . .").

capture and record the details of a person's life.[6] Already, voracious telemarketers can obtain lists of a business's customers and target those individuals with sales campaigns. With the increase in information-dependent technologies, information peddlers can obtain more intimate information about individuals with even less effort.[7] As lawmakers establish the foundation for maximizing the benefits of the coming technological explosion, they must also protect Americans from the intrusive aspect of communications and information technologies. Indeed, one member of Congress has expressly addressed the issue, by stating that legislation must establish

> prospective privacy safeguards to ensure the perpetuation of such privacy rights as communications and computer technology continue to merge and evolve. Regardless of the particular technology a consumer may use, their [sic] privacy rights should remain a constant. In short, consumers should know when personal data is being collected. They should be given proper notice if those collecting personal information intend to reuse or sell such personal data. And finally, consumers must be given the right to prohibit or curtail such practices.[8]

A recent technology, Calling Number Identification ("Caller ID"), has bolstered the collection and commercial use of information. The service enables people to see a calling party's number as soon as the telephone rings. Most states offer a call blocking option for callers who wish that their numbers remain anonymous. Callers can block calls on a per-call basis by dialing a code before each phone call they wish to block. Per-line blocking, on the other hand, automatically blocks all calls made from a particular line.

The primary advocates of Caller ID argue that the technology will allow people to screen calls, deter the number of obscene and prank telephone calls, store the number of unanswered calls, and improve the service that companies offer repeat customers.[9] Nonetheless, "[t]he same technology also has created new ways to commit telemarketing fraud and has decreased individual privacy through the disclosure of telephone numbers and the compilation

---

[6] 59 Fed. Reg. 6844.

[7] *See id.*

[8] 139 CONG. REC. E2745-46 (daily ed. Nov. 3, 1993) (statement of Rep. Edward J. Markey, introducing the Telephone Consumer Privacy Protection Act of 1933, H.R. 3432, 103d Cong., 1st Sess. (1993)).

[9] Benjamin R. Seecof, *Caller Identification: Stealing Your Name and Number*, 18 HASTINGS COMM. & ENT. L.J. 791, 793 (1991); *Consumers Win One; Court Judges Caller ID as User-Friendly*, COLUMBUS DISPATCH, Sept. 29, 1994, at 12A.

of credit, buying, and other personal information in databases."[10] Additionally, anonymous hotlines may lose their effectiveness, unlisted numbers may lose their secrecy, and professionals who work at home will reveal the numbers from which they call.[11] Despite the benefits that Caller ID may offer, the tension arising from consumer protection concerns, and issues of control over personal information have slowed its implementation.[12] The ability to block calls on a per-line basis is the minimum requirement necessary to safeguard privacy concerns.

For seven years, Caller ID operated solely on an intrastate basis. However, a recent ruling of the Federal Communications Commission ("FCC" or "Commission") mandated Caller ID's availability on an interstate basis begining April 12, 1995.[13] Overwhelming opposition to the ruling, however, forced the FCC to postpone this date.[14]

After Caller ID's introduction, the legislature of each state that adopted it carefully considered the available blocking options that would allow callers to prevent disclosure of their telephone numbers. Various states allowed callers to block calls on a per-call basis by dialing *67 before each call.[15] States that were more protective of their citizens' privacy rights, including New York, allowed per-line blocking.[16] The FCC ruling, however, abolishes per-line blocking and imposes upon all states per-call blocking for interstate calls. This Note will discuss the FCC's ill-advised preemption of state privacy interests in its regulation of Caller ID.

Part I examines the individual's right to informational privacy, which opponents of Caller ID invoke to argue that adequate privacy mechanisms must be available. Part II considers the fundamentals of the Caller ID service and illustrates the uses of information obtained through the service. Though Caller ID is a relatively inexpensive service that offers various advantages to American homeowners and businesses, it has spawned a raging de-

---

[10] Consuelo L. Kertz & Lisa B. Burnette, *Telemarketing Tug-of-War: Balancing Telephone Information Technology and the First Amendment With Consumer Protection and Privacy*, 43 SYRACUSE L. REV. 1029, 1029 (1992).

[11] Seecof, *supra* note 9, at 793.

[12] Kertz & Burnette, *supra* note 10, at 1029; Anthony Ramirez, *How 'Unlisted' is Becoming 'Kind of Listed'*, N.Y. TIMES, May 7, 1995, at F1, F10.

[13] Rules and Policies Regarding Calling Number Identification Service—Caller ID, 9 F.C.C.R. 1764, 1766 ¶ 11 (1994); Ramirez, *supra* note 12, at 1.

[14] *See* Rules and Policies Regarding Calling Number Identification Service—Caller ID, 1995 FCC LEXIS 1864 (Mar. 17, 1995).

[15] Matthew L. Wald, *Caller ID Reaches Out A Bit Too Far*, N.Y. TIMES, Feb. 2, 1995, at B1, B4.

[16] For example, callers may forget to dial the blocking code or may incorrectly dial the code.

bate over the competing privacy interests of both callers and called parties. Part III examines the FCC's ruling and criticizes the agency's justifications for preempting state privacy protections. Part IV proposes measures for providing calling parties with adequate privacy protection. Finally, part V examines the FCC's preemption of state law in the Caller ID field, and argues that the FCC's ruling contravenes congressional intent to safeguard individuals' informational privacy.

I. The Value and Dangers of Information

A 1993 Equifax survey by Louis Harris & Associates and privacy scholar Alan F. Westin revealed that seventy-one percent of Americans feel that they have lost control over personal information about themselves, while an even greater percentage worry about threats to their personal privacy.[17] This past summer the former number increased to eighty percent.[18] During the summer of 1995, six out of ten Americans surveyed said that they have refused to give information to a company because it was too nosy.[19] Despite these valid concerns, however, the effectiveness and social and economic value of current information-gathering capabilities render information technologies extremely important. Technological advancements will improve people's personal, academic, and professional lives by increasing the availability of services and information resources.[20]

Computer technology has made it possible for businesses to better serve customers by collecting intimate data about the individuals with whom they transact.[21] Often, individual profiles help companies operate more efficiently by helping them understand consumers' interests and needs. Also, the computerized storage of information makes a customer's profile readily accessible when Caller ID displays the customer's number. At the same time, the information age is creating a surveillance society in which the combination of various consumer databases results in the profiling and monitoring of individual lifestyles.[22] Private databases contain ex-

[17] Louis Harris & Assocs. & Alan F. Westin, The Equifax Report on Consumers in the Information Age 1, 10 (1993); *see* Louise M. Benjamin, *Privacy, Computers, and Personal Information: Toward Equality and Equity in an Information Age*, 13 Comm. & L. 3, 3 (1991).

[18] Bruce Horovitz, *Invasion of Privacy Consumers, You are What You Buy*, Denv. Post, Dec. 25, 1995, at A25.

[19] *Id.*

[20] *See* 59 Fed. Reg. 6843.

[21] *See* Kertz & Burnette, *supra* note 10, at 1029.

[22] David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 Case W. Res. L. Rev. 831, 835 (1991).

tensive information about people, including their spending habits, income, medical procedures, family, health, and even future vacation plans.[23] Personal information typically is gathered from a variety of records that different businesses maintain to target future solicitations and to sell the records to other businesses.[24]

With the help of Caller ID, individuals' profiles reveal all telephone numbers that they have dialed. These numbers include calls to a record store, a diet clinic, or an adult movie theater to make routine "anonymous" inquiries about hours of operation. By accessing various databases, marketers add vast amounts of information to original profiles.[25] These computer portraits allow companies to craft their marketing techniques to target a particular consumer's attitudes, values, and interests.[26] For example, the person whose profile reflects a call to a diet clinic may receive a deluge of solicitations targeting overweight people.

The commercial value of intrusive information encourages holders of large databases to constantly develop profitable ways in which to exploit the data.[27] Indeed, the direct mail industry relies for its survival upon the dissemination of personal information about individuals drawn from a variety of lists.[28] On average, a minimum of twenty-five marketing databases list each American's name.[29] After gathering heavily intrusive personal data, many companies sell the information without regard to the uses for which such information will be put.[30] From the scraps of data marketers gather about individuals, companies can create and sell mailing

---

23 *See* Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 SANTA CLARA COMPUTER & HIGH TECH. L.J. 431, 431 (1993).

24 Seecof, *supra* note 9, at 793.

25 Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1400 (1987).

26 *See id.* at 1395. Mallory Hughes, a Florida resident, recently realized the extent to which direct marketers will use personal information about individuals. JEFFREY ROTHFEDER, PRIVACY FOR SALE 23 (1992). Hughes received a letter from evangelist Oral Roberts, with whom she had no previous contact. The letter began with "Mallory, I am your Partner and your friend, and because I am so close to you in spirit, I feel I can say something very personal to you . . . ." It continued by stating, "Mallory, it's time for you to get out from under a load of debt, that financial bondage that . . . makes you feel like you have nowhere to turn. The devil tells you, 'You've made your bed of debt, now you've got to lie in it. You're going to be paying on your bills for the rest of your life. . . .' Well Mallory, I don't have a magical answer for your pile of bills and financial bondage. But I do have a miraculous answer, direct from the throne of God to your home." *Id.* No divine intervention gave Roberts the power to read Mallory's mind. Instead, "Roberts had purchased Hughes's name from one of dozens of computerized files that list suspected financial deadbeats." *Id.* at 24. Roberts shocked Mallory by urging her to send a gift of $100 to Oral Roberts, so that he could approach God on Mallory's behalf. *Id.*

27 Graham, *supra* note 25, at 1403.

28 *Id.* at 1400.

29 Horovitz, *supra* note 18.

30 Graham, *supra* note 25, at 1397.

lists organized by an infinite variety of characteristics.[31] Recent data shows the existence of more than 15,000 marketing lists containing two billion consumer names, or potential targets.[32] Resulting from such profit incentive is a booming industry involving commercial dissemination of private information. A 1990 report estimated that the sale of personal information was a three billion dollar a year industry.[33] The information is often used for reasons other than originally intended and is manipulated by those who have no prior relationship with the individual to whom the data pertains.[34] In fact, most people have no knowledge or control over what information is collected about them and how it is used.[35]

An additional problem posed by the information industry is unauthorized access to stored data. Search firms, such as the National Credit Information Network, allow subscribers with computer modems to conduct on-line searches of millions of on-line consumer and commercial credit reports, drivers' license records, and databases containing social security numbers.[36] One such Florida firm boasted that "[o]ne phone call and a credit card number puts the most intimate details of your life at the disposal of anyone willing to pay."[37]

The use of personal information to market goods and services may become even more intrusive when it falls into the wrong hands. Despite efforts to combat consumer fraud, telephone fraud

---

[31] *See* Blackman, *supra* note 23, at 431. These lists often increase the occurrence of consumer telemarketing fraud committed by boiler-room operations, which move their location as soon as suspicions heat up. Joe Wayne, *Dialing for Defendants*, CAL. LAW., Aug. 1993, at 28. Indeed, after talking with some extremely unsophisticated consumers, "[s]ome boiler-room operators even compiled lists of easy targets that were sold to other telemarketers." *Id.*

[32] Horovitz, *supra* note 18; *Consumers Win One; Court Judges Caller ID as User-Friendly*, *supra* note 9.

[33] 59 Fed. Reg. 6842.

[34] *Id.*; *see* Kertz & Burnette, *supra* note 10, at 1066.

[35] This reality is particularly troubling when one considers the possibility of erroneous information collected and disseminated. Indeed, "[p]utting information into America's invisible electronic data network is relatively easy, but getting it out—*no matter how wrong it is*, or how many people know that—can be impossible." Larry Tye, *No Private Lives: When the Cost of Information is Too High*, BOSTON GLOBE, Sept. 5, 1993, at 19 (emphasis added). An example of the disaster that can result from erroneous information is the case of Phyllis and Keith Mirocha of Louisville, KY. Trans Union, one of the three major credit reporting agencies, confused Phyllis's record with a woman who had $60,000 in bad debts. Trans Union never followed through on its promise to correct the problem. Eventually, the Mirochas "couldn't get financing for their new home, developed medical and other problems they say made it impossible to hold their jobs, and eventually lost their existing home and car." *Id.*

[36] Benjamin, *supra* note 17, at 5.

[37] Larry Tye, *No Private Lives: Hidden Assets are an Open Book to Fla. Firm*, (pt. 1), BOSTON GLOBE, Sept. 5, 1993, at 18.

remains widespread today.[38] The telephone con artist typically describes fictitious companies offering a limited, one-time only deal to participate in a phony investment scheme or purchase a revolutionary product.[39] The increased distribution of personal information makes it even easier for scam artists, whose schemes rarely deliver the promised riches or goods, to bilk unsuspecting consumers of billions of dollars each year.[40]

New telephone technologies, such as Caller ID, have furthered the potential for telemarketing fraud and the dissemination of personal information through the disclosure of consumers' telephone numbers.[41] A business's ability to record a caller's number and add to the profile information from their conversation can lead to disclosure of intimate information about an individual's tastes and interests. Therefore, any system of Caller ID must account for these consumer fraud and informational privacy concerns.

II. CALLER ID

Ever since the introduction of Caller ID, a heated debate has developed over the competing privacy rights of calling parties and call recipients.[42] Telephone companies advertised Caller ID as a miracle technology that finally enabled individuals to regain security and control in their homes.[43] Telephone companies marketed the small device, priced at between sixty and one hundred dollars,[44] as the key to identifying and preventing harassing and ob-

---

[38] *See* James A. Albert, *The Constitutionality of Requiring Telephone Companies to Protect Their Subscribers From Telemarketing Calls*, 33 SANTA CLARA L. REV. 51, 55 (1993). In March of 1993, the Federal Bureau of Investigations ended an undercover telemarketing investigation with indictments against 90 individuals and 7 telemarketing companies in California, and an additional 150 indictments elsewhere. Wayne, *supra* note 31, at 28.

[39] *See* Albert, *supra* note 38, at 54.

[40] Wayne, *supra* note 31, at 28. One notable scheme of the 1980s involved consumers who paid more than $500 million for fake Dali prints sold by telephone. In another instance, telemarketers in Florida swindled more than $75 million by telephone after offering to sell bars of gold. Actually, consumers received painted gold blocks of wood that were stored in a Florida vault. Another scheme, in which a Pennsylvania woman lost more than $100,000, involved telemarketers who informed victims that they had won a sweepstakes. The scam artists, however, required a purchase of costly merchandise in order to claim the prize. After the companies received people's money, they sent useless merchandise before disappearing. *Id.*

[41] Kertz & Burnette, *supra* note 10, at 1029.

[42] *See generally* Glenn C. Smith, *We've Got Your Number! (Is It Constitutional to Give It Out?) Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145 (1989). In the Matter of Rules and Policies Regarding Calling Number Identification Service—Caller ID, 9 F.C.C.R. 1764 (1994).

[43] *See* Smith, *supra* note 42, at 70.

[44] Rules and Policies Regarding Calling Number Identification Service, 6 F.C.C.R. 675 ¶ 2 (1992). Telephone companies also charge Caller ID subscribers a monthly fee. NYNEX currently charges $6.50 per month. Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at B1. In most states, Caller ID costs between $3.50 and $10.00 per line per month

scene telephone calls and facilitating emergency response services by making callers immediately identifiable.

Advocates argue that Caller ID will reduce the number of false alarms, fake bomb threats to schools, and other harassing and life-threatening prank telephone calls.[45] Additionally, the business community provides strong support for the service. For example, Caller ID allows a pizzeria to ensure that the telephone orders it receives are genuine.[46] A bank could allow customers to conduct more telephone transactions after entering a password, since Caller ID gives the bank greater assurance of customers' identities.[47]

Yet, Caller ID was a fertile source of controversy and discontent even before its market introduction. Battered women's shelters across the country vehemently argued that the service would endanger abused women who decide to call their husbands from the shelter.[48] Additionally, professionals who maintain client contact from their homes at odd hours, such as psychiatrists, justifiably feared that Caller ID would put their lives at risk.

A. *The Business Community's Best Friend*

In addition to these legitimate safety concerns, privacy is a concern when consumers use the telephone to contact businesses. Phone numbers increasingly are the key to cross-referencing databases of information about consumers, creating "a trend that is making our phone numbers the single most desirable bit of demographic data that corporate America can gather on us."[49] With Caller ID, businesses can greet repeat telephone callers by name

for businesses. Richard Grigonis, *Caller ID = Much Better Customer Service*, COMPUTER TELEPHONY, Feb. 1995, at 56.

[45] Steven P. Oates, *Caller ID: Privacy Protector or Privacy Invader?*, 1992 U. ILL. L. REV. 219, 230 (1992); *see* Barasch v. Pennsylvania Pub. Util. Comm'n, 576 A.2d 79, 88 (Pa. Commw. Ct. 1990), *aff'd*, 529 Pa. 523 (Pa. Super. Ct. 1992); *see also Consumers Win One; Court Judges Caller ID as User-Friendly*, *supra* note 9.

[46] Domino's Pizza, Inc. franchises ("Domino's") use the service to verify more than 200 million telephone calls daily. After reading customers' phone numbers, Domino's computers make orders more efficient by automatically retrieving the addresses. Employees are alert to callers who give different telephone numbers than those revealed by Caller ID. "Someone who is going to rob our pizza delivery driver is not going to give us a good phone number, said Don Gonos, national telecommunications manager of Domino's." Ellen Messmer, *FCC Gets Earful on Caller ID*, NETWORK WORLD, May 23, 1994, at 1; *see* Ross E. Mitchell & Judith Wagner, *Dynamic Negotiation in the Privacy Wars*, TECH. REV., Nov., 1994, at 70, ¶ 10.

[47] Matthew L. Wald, *Federal Caller-ID Rule Sparks Privacy Debate*, N.Y. TIMES, Oct. 13, 1994, at C2.

[48] *See Barasch*, 576 A.2d at 88; *Consumers Win One; Court Judges Caller ID as User-Friendly*, *supra* note 9.

[49] Carla Lazzareschi, *Phone Firms Had High Hopes for New Services, But One That Discloses a Caller's Number is Pushing a Hot Button With Caller ID*, L.A. TIMES, July 15, 1992, at 1.

and use their telephone numbers to automatically retrieve a list of their purchasing habits.[50] Then, using a personal computer, a business can obtain a caller's name, address, record of previous calls to the business, and other useful information gathered from cross-referencing various databases.[51] Marketers combine demographic data gathered from credit card records to develop an accurate profile of a consumer's purchasing habits.[52]

Caller ID pits two types of individual privacy interests against each other. The privacy of callers is weighed against the privacy of the call recipients and presents a unique balancing test.[53] With respect to the commercial information industry, companies depend on the service to know their customers. They argue that the ability to display a customer's record even before answering the phone enables them to serve their customers better by reducing the amount of information requested from that customer. At the same time, however, marketing representatives may scan the customer profiles to target the unsuspecting consumer with an individually crafted sales pitch.[54] Therefore, although Caller ID may make companies more efficient, it threatens individual privacy by adding new information about consumer preferences into companies' profiles every time consumers call.

Just because an individual calls an adult products store to make a routine inquiry about business hours does not mean that the caller wants his or her name and number on an adult film marketer's or *Penthouse's* solicitation list of libidinous consumers.[55] Marketers may sell such compelling information to others willing to pay the fee.[56] Thus, the individual's "sullen, private desires have become an open book, one that marketers are desperate to read

---

50 ANNE W. BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 43 (1994).

51 Seecof, *supra* note 9, at 795.

52 *Id.*

53 Oates, *supra* note 45, at 229.

54 Congress has expressely noted that "[u]nrestricted telemarketing . . . can be an intrusive invasion of privacy . . . ." Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394, ¶ 2 (codified as amended in 47 U.S.C. § 227 (1994)).

55 *See generally* Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at C2. Senator Herbert Kohl, Democrat of Wisconsin, stated that "[s]enators and other public officials should be able to call The Washington Post, whose reporters have caller ID on all their phones, without revealing their home phone numbers and addresses. And consumers should be able to call a business and ask for information without being compelled to identify themselves." *Congress Likely to Impose Uniform Caller ID Blocking Rule*, TELEPHONE WK., Feb. 8, 1993.

56 *See Reply to Oppositions* at 4, *Rules and Policies Regarding Calling Number Identification Service—Caller ID*, CC Docket No. 91-281 (1994) (stating that a "single phone call will have published the formerly confidential unlisted phone number in widely available lists. A number that was secret one day will be available the next for a small fee to every detective agency or telemarketer on the information super-highway.").

and digest so that they can cash in on [the individual's] propensities."[57] Worse, information of the individual's interest in adult products may become a part of his or her permanent profile, accessible to potential employers or landlords.

B. *Blocking Measures*

Before the FCC mandated interstate Caller ID, the service existed in almost every state,[58] solely for intrastate calls.[59] States actively regulated the service within their boundaries, weighing the benefits of Caller ID against the privacy interests of the caller. The available blocking options demonstrate various states' awareness of the privacy needs of the calling party.[60] Shortly before the FCC ruling, some form of a service that blocks Caller ID from revealing the originating number was available in over forty states.[61]

Per-line blocking is perhaps the strongest weapon against Caller ID.[62] It allows individuals to bar disclosure of all calls originating from a particular subscriber's line.[63] An individual wishing to deactivate the block to reveal their telephone numbers to the called party can dial an unblocking prefix before dialing the telephone number.[64] Some of the individuals relying upon per-

---

57 ROTHFEDER, *supra* note 26, at 16.

58 *See* Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at C2.

59 Interstate Caller ID depends upon interconnection of the local exchange carriers' SS7 networks with interexchange carriers' SS7 network, in order to allow the transmission of the caller's number from the originating to the terminating end of the call. Even after the FCC's ruling, interconnection did not occur immediately. Therefore, for many months nationwide, Caller ID was unavailable in any state. 6 F.C.C.R. at 6752 ¶ 4. For a discussion of the continued unavailability of interstate Caller ID, see *infra* notes 80-82 and accompanying text.

60 *NARUC Communications Committee Vice Chairman Tells Congress to Consider Setting National Standard on Caller ID Services and Blocking*, RBOC UPDATE, Aug. 1993.

61 Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at C2 (stating that as of October 1994, some form of the blocking service is available in forty one states); *States Prepare to Battle With FCC on Interstate Caller ID Rules*, 13 F.C.C.R. 12 (1994) (stating that as of June 1994, at least 43 states offered per-line blocking at least for some callers).

62 Even per-line blocking, however, will not necessarily protect individuals' privacy interests adequately. Recently, a scandal erupted when a telephone company error at NYNEX deprived up to 30,000 customers of promised privacy protection. Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at B1. In what privacy protection experts referred to as the only "lapse on such a large scale anywhere," for about a year, NYNEX transmitted to the called parties the numbers of as many as 30,000 customers who thought they had activated per-call blocking or per-line blocking. *Id.* NYNEX provided no explanation for the failure and offered telephone numbers free to the people it failed to protect. *Id.*

63 Rules and Policies Regarding Calling Number Identification Service, 6 F.C.C.R. 6752 ¶ 2 (1991).

64 Typically, the unblocking code required is *67. Mitchell & Wagner, *supra* note 46, at 70. This is problematic when the same code is required to utilize the per-call blocking function. The command has different functions on different telephones, leading to confusion in various circumstances. *See* Wald, *Federal Caller-ID Sparks Privacy Debate*, *supra* note 47, at C2. For a discussion of the confusion that the blocking and unblocking codes cause, see *infra* notes 132-33 and accompanying text.

line blocking include teachers at home who wish to call students, doctors who must call patients from their homes, and undercover police officers working from home to monitor suspects. For example, an investigator for the New York State Consumer Protection Board relies upon per-line blocking when she uses her home phone in investigations.[65] Additionally, an Albany man working as a skip tracer, tracking people that have jumped bond, requested per-line blocking in order to effectively perform his job. Many states, including New York, allowed per-line blocking after concluding that per-call blocking was too burdensome for many such individuals.[66] Results from the National Association of State Utility Consumer Advocates ("NASUCA"), compiled shortly before the FCC ruling, show that twenty-nine states offer per-line blocking either for free or for a charge, while fourteen states make per-line blocking available only to special groups that can demonstrate a compelling need for privacy.[67]

The second blocking option is per-call blocking, which is available in most states.[68] Telephone users wishing to conceal their identities must dial *67 before every call. If they forget to enter this special code when dialing a Caller ID subscriber (not an unusual occurrence), they inadvertently forfeit their anonymity. Per-line blocking better protects callers' privacy interests, because it automatically blocks calls by default. The worst that can happen with per-line blocking is that the number of a caller who forgets to enter the unblocking code will be blocked. With per-call blocking, however, a caller who forgets to activate call blocking would mistakenly sacrifice anonymity.

III. FCC RULING

The FCC waited until seven years after the introduction of Caller ID to regulate interstate Caller ID under the Communications Act of 1934, which grants the FCC authority to regulate "all interstate and foreign communications by wire."[69] The Commission stated that "a consistent, nationwide interstate policy will contribute to economic growth as businesses employ the new technology for a number of uses . . . [including] pay-per-view televi-

---

65 Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at B1.

66 *See id.* at B4.

67 *States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61; *see* 9 F.C.C.R. 1770 ¶ 40 (indicating that certain types of law enforcement personnel may have greater privacy needs than others).

68 Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at B4.

69 47 U.S.C. § 152(a) (1988); *see* Gen. Couns. Mem., 9 F.C.C.R. 1764, 1776 § IV (1993).

sion, order/entry verification, voice messaging storage, customized customer service," and emergency service dispatch.[70]

Seeking to "[balance] the reasonable privacy expectations of both the calling and called parties and [remove] obstacles to the development of calling party based services,"[71] the Commission preempted state blocking rules by effectively banning per-line blocking.[72] Under the FCC ruling, interstate Caller ID service only will allow blocking on a per-call basis. The order explicitly stated that for intrastate calls states may not employ a blocking alternative to per-call blocking.[73]

The order does not expressly affect intrastate calls[74] and still allows states to continue to offer per-line blocking for calls originating and terminating interstate. In practice, however, compliance with the per-call blocking mandate for interstate calls prevents a state from using per-line blocking.[75] Compliance with the ruling requires that every state either comply with the federal model of per-call blocking or that carriers distinguish between interstate and intrastate calls.[76] In a recent statement, however, the U.S. Telecommunications Association noted that "[i]t's not technically possible for today's net switches to distinguish between originating interstate and intrastate calls for purposes of applying different privacy blocking protocols . . . ."[77] Thus, telephone companies are unable to offer different blocking options for interstate and intrastate calls.[78] Furthermore, prohibitive costs may prevent carriers from implementing the technology if it becomes available.[79] Citizens in states with blocking features that offer callers more privacy, such as per-line blocking, may lose such privacy rights under the FCC mandate.

---

[70] *Caller ID to be Available Nationwide: FCC Adopts Federal Policies for Regulation*, 1994 FCC LEXIS 995 (Mar. 8, 1994).

[71] *Id.*

[72] *States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61; see *Update On Interstate Caller ID: Maybe the Issue is Settled, Maybe It's Not*, ADVANCED INTELLIGENT NETWORK NEWS, Aug. 10, 1994.

[73] 9 F.C.C.R. at 1775-76 ¶ 69.

[74] *LECs and IXCs Clash Over Interstate Caller ID Order*, ADVANCED INTELLIGENT NETWORK NEWS, Sept. 7, 1994.

[75] *See* Messmer, *supra* note 46 (noting that state regulators warned that the FCC ruling has provoked a constitutional crisis); *Update on Interstate Caller ID: Maybe the Issue is Settled, Maybe It's Not*, *supra* note 72; Victor J. Toth, *Telephone Privacy—How to Invade it; Caller Identification and Automatic Number Identification*, BUS. COMM. REV., Apr. 1994, § 1, at 70; *States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61; *LECs and IXCs Clash Over Interstate Caller ID Order*, *supra* note 74.

[76] *States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61.

[77] Messmer, *supra* note 46, at 1.

[78] *See LECs and IXCs Clash Over Interstate Caller ID Order*, *supra* note 74.

[79] *Id.*

The FCC extended the deadline for compliance with the ruling from April 12, 1995, to December 1, 1995, after receiving a deluge of petitions for reconsideration of the ruling.[80] Although some carriers met the deadline for implementing interstate Caller ID, others cited technical problems and privacy concerns in support of their petitions to stay the order.[81] Faced with such opposition, the FCC again granted an extension to disgruntled petitioners until May 31, 1996.[82]

A. *Reasons for the FCC Ruling*

After stating that per-line blocking "should not be so burdensome to the service that it destroys its value and . . . fails to take into account the privacy needs of the called party" to identify a caller before answering a call, the FCC failed to adequately consider the privacy needs of callers.[83] The ruling states that:

> [i]n the [Notice of Proposed Rulemaking], we tentatively concluded that per line blocking unduly burdens calling party number based services overall by failing to limit its applicability to those calls for which privacy is of concern to the caller. The Commission noted that even in the case of law enforcement personnel, there may be a need to maintain calling number privacy on some calls, but that the same number may be used to telephone other law enforcement personnel, victims of crimes, cooperative witnesses, and family or friends. The Commission asserted that in these types of calls, calling number privacy is not needed and calling number identification can actually be a valuable piece of information for both the caller and called parties . . . . We find that the availability of per call unblocking does not cure the ill effects of per line blocking. Moreover, in an emer-

---

80 *Rules and Policies Regarding Calling Number Identification Service—Caller ID*, 1995 FCC LEXIS 1864 (Mar. 17, 1995); *A Patchwork of Rules and Regs Tempers Many '95 Telco Plans (Part II)*, TELCO BUS. REP., Dec. 18, 1995; *see States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61.

81 *Interstate Caller ID Pack Limps Across Finish Line, But Some Stragglers Remain*, WASH. TELECOM NEWS, Dec. 18, 1995 (stating that whether information about interstate callers was transmitted depended on from where the call originated and the carrier). Although some carriers provided interstate Caller ID service by the December 1 deadline, not all carriers abolished per-line blocking in compliance with the deadline. *See* Raymond Fazzi, *Caller ID Makes National Connection; Changes Won't Increase Service Fees*, ASBURY PARK PRESS, Dec. 2, 1995, at C7; Stephen Keating, *Caller ID Going National Today, With Safeguards*, DENV. POST, Dec. 1, 1995, at D2; John Kirkpatrick, *Caller ID Now to Cover Long-Distance*, DALLAS MORNING NEWS, Dec. 1, 1995, at 1A. *But see* COMM. DAILY, Dec. 1, 1995, at 8 (stating that the only blocking option nationwide is per-call blocking); BELL ATLANTIC, SEE THE PHONE NUMBERS OF YOUR INCOMING CALLS—MADE FROM ANYWHERE IN THE USA! (1996) (on file with the *Cardozo Arts & Entertainment Law Journal*).

82 *Id.*; *see FCC Permits Caller ID Delay*, STATE TELEPHONE REG. REP. (Telecom Publishing Group, Foster City, CA), Dec. 14, 1995.

83 9 F.C.C.R. at 1764 ¶ 46.

> gency, a caller is not likely to remember to dial or even to know to dial an unblocking code. For the foregoing reasons, we find that a federal per line blocking requirement for interstate [calling party number] based services, including caller ID, is not the best policy choice of those available to recognize the privacy interests of callers.[84]

Additionally, the FCC states that "[a]s a matter of simplicity and uniformity, per call blocking allows callers to travel from phone to phone and make an informed privacy decision. Per-line blocking may create caller confusion when a caller uses a phone and is uncertain whether it is equipped with per-line blocking."[85] Essentially, the Commission's reasoning is that "per-line blocking is a bad idea because subscribers are [not smart enough] to unblock calls when they want to unblock them, although [they are smart enough] to block calls when they want to block them."[86] It appears that the Commission's true motivating factor in establishing Caller ID with minimal privacy protection is that the service "promises important efficiency and productivity gains for our economy."[87] While interstate consistency and a thriving economy are laudable goals, they do not justify neglecting individuals' privacy and safety interests.

B. *Problems with the FCC Ruling*

Not surprisingly, the FCC ruling provoked immediate, angry responses from fourteen states, NASUCA, the Hawaii Office of Consumer Protection, and the National Administration of Consumer Agency Administrators.[88] In summarily concluding that "automatic per call blocking best addresses the privacy needs of both the calling and called parties,"[89] the FCC in its ruling "[reopened] issues of safety and privacy settled long ago by individual states."[90] State residents who currently subscribe to per-line blocking have come to expect and rely upon this level of privacy protection.[91]

---

[84] *Id.* at 1771 ¶ 43.

[85] *Id.* at 1771-72 ¶ 47.

[86] John R. Levine, *FCC Order On Interstate Caller ID*, TELECOM. DIG., May 11, 1994, *available on Internet.*

[87] *See* 9 F.C.C.R. at 1772 ¶ 48; Ramirez, *supra* note 12, at 1.

[88] *States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61.

[89] *See* 9 F.C.C.R. at 1771 ¶ 46.

[90] *States Open Major Offensive to Reverse FCC on Per-Line Blocking*, STATE TELEPHONE REG. REP. (Telecom Publishing Group, Foster City, CA), June 2, 1994.

[91] Responding to the FCC's preemption of state regulatory authority, John Rushing, a senior system engineer from Westmont, Illinois, stated: "My level of concern is always heightened whenever a federal agency usurps or limits the rights of states to self government . . . . [S]tates should be able to regulate themselves without interference from the federal government." *Cyberspeak: Voices from the Reader Network; Do You Have Any Privacy*

States that do not yet offer per-line blocking may wish to do so in the future, and the FCC ruling precludes residents of these states from ever having the opportunity to enjoy heightened privacy protection. Indeed, Ric Loll, president of TechnoMage Consultants in Illinois, states:

> I object to the FCC action. I have serious concerns about caller ID and have gone to some lengths to make sure my phone number gets limited distribution. . . . Per-line blocking (which is not yet available in my area) would be an excellent option. I don't want my phone number to get wide distribution, I get too many "cold-contact" business calls already. I can barely stand having a bell in my house, which anyone in the world can ring . . . . I prefer not to give the world the number at the same time![92]

The Commission acknowledges that women who call their husbands from domestic violence shelters require the confidentiality of shelters' numbers as a life-preserving measure.[93] Specifically, many domestic violence victims stay at homes of friends or family. Caller ID threatens the victims' safety because it allows the abusers to locate the victims.[94] Adetoun Onabanjo, the director of the Brooklyn Center for Elimination of Violence in the Family, advises all women who move out of the shelter to use a blocking service.[95] Since abused women often must contact their estranged partners, blocking Caller ID will help prevent the violence from escalating.[96]

The FCC ruling recognizes that law enforcement personnel frequently require anonymity to effectively perform their jobs.[97] The Commission also mentions that inadequate blocking services may thwart attempts to keep unlisted numbers confidential, as well as the numbers of professionals who work from their homes.[98] Indeed, the Commission actually agrees that "certain uses of captured calling numbers need to be controlled."[99] Nonetheless, the FCC failed to give these and other compelling concerns the consid-

---

Concerns as a Result of an FCC Ruling on Caller ID that Preempts State Regulatory Authority and Bans Per-line Call Blocking?, NETWORK WORLD, May 30, 1994, at 7.

92 *Id.*

93 9 F.C.C.R. at 1769 ¶ 31.

94 *Reply to Oppositions*, *supra* note 56.

95 Wald, *Caller ID Reaches Out a Bit Too Far*, *supra* note 15, at B4. According to Ms. Onabanjo, the abuse does not cease after a women leaves her husband. *Id.* Call blocking will help minimize confrontations. *See id.*

96 *Id.* A woman who shares custody of her children is one example of a victim of domestic violence who might call her abusive husband or boyfriend.

97 9 F.C.C.R. at 1771 ¶ 43.

98 *Id.*

99 *Id.*

eration they deserve. Instead, "it reached deep within the bowels of the organization and pulled out an order that seems to serve no purpose other than to take people by surprise."[100]

The Commission summarily concludes that per-line blocking is "so burdensome to the service that it destroys its value and thus fails to take into account the [actual] privacy needs of the called party," since some calls may inadvertently be blocked when the caller has no privacy concerns.[101] The FCC's record reflects little analysis and ignores that each state has had seven years to consider specific privacy concerns of its residents and select the blocking option which best balances the interests of callers and recipients. The Commission assumes that telephone subscribers can train all of their children and houseguests to dial *67 before every call.[102] Additionally, it nonsensically dismisses the privacy interests of individuals with unlisted numbers by noting that the only people who may capture an unlisted number are those that the caller has decided to call without call blocking.[103] This argument misses two points: that a caller may inadvertently forget to activate per-call blocking, and that the captured number may subsequently be sold to telemarketers. The boom in the information and telemarketing industries resulting from Caller ID should remind the Commission that the recipient marketer in turn is likely to sell the caller's number along with personal identifying information to other marketers.[104]

Per-call blocking is not a sufficient answer for various groups and individuals whose function, existence, or well-being depend upon the ability to withhold their telephone numbers from call recipients. Per-call blocking's effectiveness depends upon the assumption that all callers will be educated about how to invoke privacy protections different from those to which they have already become accustomed. Also, telephone subscribers and all other telephone users must remember how and know when to dial the code before each of the numerous calls for which the caller expects anonymity.

The FCC attempts to placate opponents of the uniform per-call blocking rule by expounding the benefits of equipment that automatically inserts the blocking code for each outgoing call on a

---

[100] Toth, *supra* note 75, at 70.
[101] 9 F.C.C.R. at 1771 ¶ 46.
[102] Carl Page, *FCC Attacks*, PRIVACY FORUM DIG., May 6, 1994, *available on Internet.*
[103] 9 F.C.C.R. at 1771 ¶ 43.
[104] *See* Seecof, *supra* note 9, at 793.

particular line, in effect creating per-line blocking.[105] The Commission simply states that those "individuals wishing to install these devices and thereby screen all originating interstate calls may elect to do so."[106] Furthermore, the Commission reasons that since those who want a per-line blocking-type of service will have to purchase the devices, people will more seriously contemplate whether they truly need per-line blocking.[107] Yet, the "devices are not reliable enough to be used to protect personal safety, and . . . relying upon them is inherently discriminatory because of a deficit of multilingual customer education and technical knowledge"[108] about such equipment. Furthermore, although the cost of fourty dollars per unit seems to be insignificant to the bureaucrats,[109] it would not be financially feasible for large organizations, such as a not-for profit domestic violence shelter operating many phone lines, to install the device on each line. Low-income individuals may be unable to purchase the device, thus becoming deprived of a privacy right available to wealthier citizens.[110]

The variety of groups and individuals that require per-line blocking defy categorization.[111] Thus, the FCC correctly concluded that per-line blocking available only to special-needs groups is not an optimal alternative.[112] Such a program would require the federal government and carriers to elevate certain privacy interests over others. Additionally, offering per-line blocking only to special needs groups ignores the fact that individuals also have strong privacy interests in their telephone numbers, particularly in situations regarding disclosure to marketers.[113]

A valid concern that the FCC notes with making both per-line and per-call blocking available is that carriers use the same code to block calls on a per-call basis as that used to unblock calls on per-line blocked phones.[114] A caller may inadvertently disable the pri-

---

105 *See* 9 F.C.C.R. at 1772 ¶ 48; *Hide-and-seek with Caller ID Not Just Local Anymore and Now There's a Way to Avoid Putting Privacy on the Line*, REC., Dec. 1, 1995, at B1 (stating that stores are selling devices that simplify blocking and unblocking, some of which are built into new telephones).

106 *Id.*

107 *Reply to Oppositions*, *supra* note 56.

108 *Id.*

109 *See* 9 F.C.C.R. at 1772 ¶ 48 (stating that "[s]uch devices are available for *as little* as $40.00 per unit" (emphasis added)).

110 *See generally Reply to Oppositions*, *supra* note 56, at 13.

111 *Id.*

112 *See* 9 F.C.C.R. at 1770 ¶ 40.

113 For a general discussion of individuals' privacy and publicity rights in their telephone numbers, see Seecof, *supra* note 9, at 802-09.

114 9 F.C.C.R. at 1771-72 ¶ 47.

vacy indicator on a line that is already blocked for all calls.[115] For example, a doctor calling patients from her home might dial *67 before each call in order to activate per-call blocking. Later, she might dial *67 if calling a patient from her friend's home. However, if the friend's line is per-line blocked already, dialing *67 would inadvertently disable the blocking function and release the friend's number to the patient. Indeed, needless confusion may result from use of the same code for both blocking and unblocking.

Yet again, however, the Commission fails to consider viable solutions that would preserve the interests of all involved. Instead, the FCC immediately outlaws per-line blocking and concludes that "[a]utomatic per call blocking is easily used on a ubiquitous interstate basis, and eliminates [such] customer confusion."[116] Oddly, the simple solution of requiring a different code for blocking than unblocking did not occur to the Commission.[117] Indeed, a recent pamphlet published by NYNEX and included in every customer's phone bill, educated those customers about the new options of *67 for blocking and *82 for unblocking.[118]

Some opponents of per-line blocking, such as the telephone companies who sell the Caller ID service, fear that the use of per-line blocking will decrease the utility of Caller ID and discourage call recipients from using the service.[119] For example, Edward Young, vice president-federal regulatory and associate general counsel for Bell Atlantic, has noted that deployment of Caller ID is not as great in states that offer per-line blocking.[120] The evidence from Nevada, however, reveals the opposite. Despite the availability of absolute per-line blocking in the state, Nevada had one of the

---

115 *Id.; see States Prepare for Battle With FCC on Interstate Caller ID Rules, supra* note 61.

116 *See* 9 F.C.C.R. at 1772 ¶ 47.

117 The only reason that the Commission adopted the *67 code for per-call blocking is that they "not[ed] that the majority of jurisdictions using this method on a local basis are using *67 . . . as the dialing digits . . . ." 9 F.C.C.R. at 1771 ¶ 46. The Commission just as easily could have selected a different code for per-line blocking. The Commission employed the identical code as a matter of convenience rather than necessity.

118 The pamphlet stated that

> [n]ow there are two dialing codes to help you manage the display of your telephone number when placing calls in areas where *Nynex Call ID Service* . . . [is] available . . . . By dialing *67 *before* each call you make, you can always "block" your number from appearing on a Call ID device . . . . By dialing *82 (Per-Call Display) *before* each call you make, you can always "unblock" your number (that is, allow it to appear on a Call ID device).

NYNEX, *Nynex Extra!*, Jan. 1995 (on file with the *Cardozo Arts & Entertainment Law Journal*).

119 *See* Mary M. Adu & Gretchen Dumas, *Privacy in Telecommunications—A California Perspective*, 15 HASTINGS COMM. & ENT. L.J. 417, 438 (1993).

120 *Markey Panel Accuses Caller ID Services of Privacy Invasion*, ADVANCED INTELLIGENT NETWORK NEWS, July 7, 1993.

highest rates of Caller ID deployment in the country.[121] Additionally, Peter Bradford, the chairman of New York's Public Service Commission, noted that it has not received any complaints about the state's per-line blocking option since its introduction two years ago.[122] In any case, even if per-line blocking decreased the use of Caller ID, such a trend might simply evidence the overwhelming number of individuals and organizations who depend upon and expect privacy protection from Caller ID.

The FCC's focus on commerce and economic development[123] to the exclusion of individual privacy interests is misguided.[124] The Commission, dazzled by the possibility that the "passage of the calling party number can promote technological innovation and new applications that will foster economic efficiency and provide new employment, manufacturing and investment opportunities,"[125] automatically places the countries' economic advancement before individuals' fundamental interests.

IV. A Proposal to Preserve the Privacy Interests of Callers

According to the National Association of Consumer Agency Administrators, the FCC's elimination of per-line blocking "compels an unnecessary invasion for millions of telephone users"[126] by failing to adequately consider public safety interests and privacy needs. Requiring a *minimum* standard of free per-call blocking, but allowing states to individually offer greater privacy protection like per-line blocking, more fairly balances the interests of both callers and recipients. Additionally, such a measure accounts for the probability that "it would be reactionary to withdraw features such as line blocking that have already been instituted to provide public safety and privacy."[127] Although the Commission claims that it minimized public confusion by instituting a policy of only per-call blocking, "the FCC is the one creating confusion by attempting to propose a single national caller ID blocking standard on the states

---

121 Adu & Dumas, *supra* note 119, at 439.

122 *States Prepare for Battle With FCC on Interstate Caller ID Rules, supra* note 61.

123 The market for Caller ID in the United States is thriving. Forecasters expect the United States market for the systems "to exceeded [sic] $175 million by 1995, compared with $50 million in 1993, according to Montgomery Securities." Brian Finnerty, *Cidco Inc.*, Investor's Bus. Daily, Sept. 2, 1994, at A4. The sales of Cidco, the leading provider of Caller ID devices, reported an increase of 123% in net income in 1993, after losing money the previous year. *Id.*

124 *See* Wald, *Caller ID Reaches Out a Bit Too Far, supra* note 15, at B1.

125 9 F.C.C.R. at 1766 ¶ 8.

126 Messmer, *supra* note 46, at 1 (quoting a statement made by the National Association of Consumer Agency Administrators); *see States Prepare for Battle With FCC on Interstate Caller ID Rules, supra* note 61.

127 *Reply to Oppositions*, *supra* note 56, at 1.

after years of federal inaction."[128]

One of the FCC's few valid criticisms of per-line blocking is that in an emergency, a caller is unlikely to remember to dial the *67 unblocking code.[129] The inability to immediately identify those who require emergency services certainly can threaten public health and safety. Once again, however, the Commission failed to consider solutions and instead robotically concluded that they must ban per-line blocking. A simple solution would be to disable call blocking to certain emergency services. The FCC is aware of this answer, as evidenced by their decision to disable all call blocking on calls to a public agency's emergency line, a poison control line, or in conjunction with 911 emergency services.[130] By similarly deactivating call blocking on calls to services such as police stations and hospital emergency lines, as well as poison control lines not belonging to public agencies, the FCC would eradicate any problem presented by the blocking of emergency telephone calls.[131]

Emergency services that justify disabling call blocking on incoming calls are those services that people would call in life-threatening situations when they require immediate help. In such exigent circumstances, it is imperative that the emergency service identifies the ill or frantic caller as quickly as possible. Given this definition, it will not be overwhelmingly difficult to accurately classify most emergency services.

As the FCC acknowledged, potential confusion exists in states where the code *67 both unblocks per-line blocking and activates per-call block.[132] Allowing state blocking and unblocking mechanisms in the call's originating end to control the information transmitted to the terminating end will mitigate the problem, since individual subscribers will know which blocking option is on their lines. Unfortunately, inadvertent unblocking of calls on per-line blocked lines may still occur. For example, the victim of domestic violence who flees to the homes of various friends and family may not know whether each home has per-line or per-call blocking. A

---

128 *States Prepare for Battle With FCC on Interstate Caller ID Rules*, *supra* note 61.

129 9 F.C.C.R. at 1771-72 ¶ 47.

130 *Id.* at 1770 ¶ 37.

131 Such a proposal is administratively feasible, even though questions may occasionally arise regarding certain entities' emergency service status. For example, it is unclear if a battered women's hotline is an emergency service that justifies disabling call blocking for incoming calls. Additionally, some argue that disabling call blocking mechanisms for calls to suicide prevention hotlines may discourage potential suicide victims from calling for help. *See* Herbert Buchsbaum, *No Secrets in Cyberspace? Computers and Privacy Rights*, SCHOLASTIC UPDATE, Sept. 2, 1994, at 11.

132 9 F.C.C.R. at 1771 ¶ 47; *see LECs and IXCs Clash Over Interstate Caller ID Order*, *supra* note 74.

different prefix for unblocking calls than for blocking would eliminate the confusion that the universal toggling code creates.[133] These two codes must be consistent throughout the country.

When an individual wishes to block a call and is unaware of which blocking option to use, the carrier should provide guidance. For example, if the person dials *67 on a line which is already per-line blocked, a recorded message should instruct the caller that the subscriber has per-line blocking and no code is necessary to block the call. On the other hand, if the caller dials the unblocking code instead of *67 on a per-call blocking line, the message should similarly convey that the individual must dial *67 to block a call. This system allows individuals using other people's phones to protect the phone owner's privacy and safety with minimal effort.

A. *Consumer Education*

The FCC agrees that "no segment of the calling public can adequately control dissemination of the calling number under any regulatory structure if they are unaware that their calling number is being identified."[134] Consumer education regarding implementing available privacy options will help prevent inadvertent forfeiture of individuals' rights. Carriers should be responsible for educating consumers about invoking the various blocking mechanisms. To make fully informed decisions regarding their privacy interests, however, it is critical that customers also understand how information from their telephone calls can become part of a computer profile of each individual, created by combining databases of personal information. Significantly, therefore, carriers must educate consumers that marketers may use Caller ID information in order to compile lists of potential customers. Furthermore, the carriers should advise their customers that companies may sell these lists to telemarketers.[135]

The fact that Caller ID can be used against a telephone customer demands that carriers provide clear and conspicuous disclosure pamphlets with telephone bills. Customer education, however, should not be limited to these types of mailings or the fine print contained in the subscriber's initial contract. Callers' compelling privacy and safety interests require that carriers also utilize more pervasive forms of advertising, such as television commercials and magazine advertisements. Additionally, such adver-

---

133 For example, the code for blocking can be *67, while the universal code for unblocking can be *82. *See* NYNEX, *supra* note 118.

134 9 F.C.C.R. at 1774 ¶ 59 (citation omitted).

135 *See* Buchsbaum, *supra* note 131, at 11.

tisements must be available in other languages, so that the non-English speaking population can adequately assess its privacy interests.[136]

The Local Exchange Companies ("LECs") should be responsible for paying for consumer education, since the LECs are the ones who profit from providing Caller ID.[137] If the advertising expenses prove unduly burdensome for the LECs, the compelling privacy and safety concerns of Americans justify a government subsidy.

B. *Per-Call Blocking as a Minimum Standard*

Over time, public debate about Caller ID and federal silence regarding the privacy and safety issues posed encouraged states to regulate the service.[138] Before the FCC preempts the states' careful considerations regarding the service, the Commission should more fully investigate the details of each state's belabored decision. Significantly, most states initially adopted proposals much like the FCC's current order, but determined that greater public safety and privacy protections were necessary.[139] "The FCC [did not consider] a new situation, it [merely reconsidered] an issue that has been *more carefully* considered before."[140] Surely, each state's painstaking consideration of its own citizens' unique privacy interests and organizations' safety interests requires deference.

The FCC, however, should not defer to those states that offer no blocking option. Requiring these states to offer a minimum privacy protection standard of per-call blocking is a legitimate imposition. Approving Caller ID with no blocking mechanism could only be justifiable if it is found that the calling parties' interests are substantially negated or nonexistent. Nothing, however, indicates that the recipient's interest in thwarting prank or obscene phone calls and facilitating customer service is so strong that it negates the caller's interests. Indeed, the immediate opposition to the FCC's ruling from various organizations and entities across the country

---

136 *But cf.* Oates, *supra* note 45, at 241 (arguing that to render Caller ID constitutional, the telephone company need only take reasonable steps to notify customers of blocking options).

137 The FCC order requires long distance carriers to pass calling party number information to the terminating LECs for free. *LECs and IXCs Clash Over Interstate Caller ID Order*, *supra* note 74. The ruling has been a source of bitter debate for the long distance carriers, who argue that the order violates the Fifth Amendment by depriving them of the ability to charge for services provided. *Id.*

138 *See Reply to Oppositions*, *supra* note 56.

139 *Id.* at 5. "The main difference between the FCC's deliberations and the states [sic] is that the FCC has so far not had the benefit of real information from real customers about their real personal safety issues." *Id.*

140 *Id.* (emphasis added).

establish that calling parties have at least some privacy interests. Therefore, the existence of privacy and safety interests of callers requires at least a minimum standard of call blocking.

V. The FCC's Preemption of State Law

A. *Congress's Power to Preempt State Law*

The Supremacy Clause of the United States Constitution establishes the supremacy of federal laws over those of the states.[141] Under traditional federal preemption doctrine, federal law preempts state law in several instances.[142] State law must yield if Congress either explicitly or implicitly intends to occupy a field.[143] In this circumstance, federal law is so pervasive that it leaves no room for states to supplement, regardless of any clash or agreement with the federal statute.[144] Federal preemption also occurs if a state regulation makes it impossible to comply with both a state and federal law, or when state law inhibits the full purposes and objectives of Congress.[145] Finally, the federal interest in the field may be so dominant that courts will presume that federal regulation precludes enforcement of state laws in the same field.[146]

The Supreme Court expressly has recognized that regulations promulgated by a federal agency, acting within the scope of its congressionally mandated authority, have the full force of federal law.[147] Thus, regulations of an agency, such as the FCC, can displace state laws in the same way as do congressional enactments.[148]

---

141 U.S. Const. art. VI, § 2.

142 Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1946); *see* Mary Ann K. Bosack, Note, *Cigarette Act Preemption—Refining the Analysis*, 66 N.Y.U. L. Rev. 756, 766 (1963).

143 Silkwood v. Kerr McGee Corp., 464 U.S. 238, 248 (1984); *Rice*, 331 U.S. at 230; Hines v. Davidowitz, 312 U.S. 52, 66 (1940); Daryl R. Hague, Note, *New Federalism and "Occupation of the Field": Failing to Maintain State Constitutional Protections Within a Preemption Framework*, 64 Wash. L. Rev. 721, 722 (1989); *see* Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355 (1986).

144 *Rice*, 331 U.S. at 230; Hague, *supra* note 143, at 722.

145 *Louisiana*, 476 U.S. at 368; *Silkwood*, 464 U.S. at 248; *Rice*, 331 U.S. at 230 (stating that preemption occurs if "the state policy [produces] a result inconsistent with the objective of the federal statute").

146 *Rice*, 331 U.S. at 230.

147 *Louisiana*, 467 U.S. at 369 (stating that "[p]re-emption may result not only from action taken by Congress itself; a federal agency acting within the scope of its congressionally delegated authority may pre-empt state regulation") (citations omitted).

148 *Id.*; Hague, *supra* note 143, at 722-23. Some refer to executive agencies as a fourth branch of government that is not directly affected by the electorate. *See* Federal Trade Comm'n v. Ruberoid Co., 343 U.S. 470, 487 (1952) (Jackson, J., dissenting) (noting that the most important modern trend is the creation of government agencies, the fourth branch of government).

B. *The Validity of Agency Rules that Preempt State Law*

Federal agencies may, without express congressional approval, issue regulations that preempt state laws.[149] When a state contests an agency's preemption of state law, however, the pivotal consideration in reviewing a regulation is congressional intent.[150] In *Chevron United States, Inc. v. Natural Resources Defense Council, Inc.*,[151] the United States Supreme Court established a two-part test focusing on whether "Congress has . . . directly spoken to the precise question at issue . . . ."[152]

In the first prong of the test, the reviewing court searches for express Congressional intent.[153] If Congress unambiguously has manifested its intent or explicitly empowers an agency to enact a particular regulation, both court and state must defer to federal regulation in that area.[154] Courts require a permissible construction of a statute when Congressional intent is ambiguous.[155]

Courts need not interpret the statute or conclude that the agency's construction was the most effective one that it could have adopted.[156] The paramount consideration instead is the reasonableness of the agency's regulation and whether the agency exceeded its statutory power.[157]

> Where Congress has directed an administrator to exercise his discretion, his judgments are subject to judicial review only to determine whether he has exceeded his statutory authority or acted arbitrarily . . . . If [h]is choice represents a reasonable accommodation of conflicting policies that were committed to

---

149 Lincoln Sav. & Loan Ass'n v. Federal Home Loan Bank Bd., 856 F.2d 1558, 1560 (D.C. Cir. 1988).

150 *Louisiana*, 476 U.S. 355; Michael R. Bergmann, Note, *Regulatory Overrides of State Antibranching Statutes: Of More Valuable Thrifts and Administrative Policy*, 77 VA. L. REV. 1203, 1213 (1991); *see Hines*, 312 U.S. at 66-67.

151 467 U.S. 837, 837 (1984).

152 *Id.* at 842. *Chevron* involved legislation establishing a permit program for stationary sources of air pollution. *Id.* According to the legislation, plants could only obtain permits for "stationary sources" if they complied with several stringent conditions. At issue was the Environmental Protection Agency's ("EPA's") plantwide definition of the term "stationary source," which enabled a plant with several pollution-causing devices to install one source without meeting permit conditions if such addition would not increase the total emissions from the plant. The Natural Resources Defense Council challenged the EPA's plantwide definition of "stationary source." After determining that Congress had no specific intent regarding the broad definition, the Court upheld the use of the EPA's concept as a reasonable policy choice. *Id.* at 842.

153 *Id.*; Bergmann, *supra* note 150, at 1214.

154 *Chevron*, 467 U.S. at 842-43; Bergmann, *supra* note 150, at 1214.

155 *Chevron*, 467 U.S. at 843.

156 *See id.* at 844 (stating that if the legislative delegation of power to an agency is implicit, "a court may not substitute its own construction of a statutory provision for a reasonable interpretation made by the administrator of an agency").

157 *Id.* at 843.

> the agency's care by the statute, we should not disturb it unless it appears from the statute or its legislative history that the accommodation is not one that Congress would have sanctioned.[158]

Additionally, an agency has no power to act until Congress confers power upon it.[159]

C. *Case Law Regarding the FCC's Statutory Authority*

The FCC derives its authority to regulate Caller ID from the Communications Act of 1934, which grants the Commission power to develop and regulate "interstate and foreign commerce in wire and radio communication."[160] Congress initially envisioned a system in which the FCC would regulate interstate telecommunication services, while the states controlled intrastate telecommunications.[161] In a short time, however, it became apparent that

> while the Act would seem to divide the world of domestic telephone service neatly into two hemispheres—one comprised of interstate service, over which the FCC would have plenary authority, and the other made up of intrastate service, over which the States would retain exclusive jurisdiction—in practice, the realities of technology and economics belie[d] such a clean parceling of responsibility.[162]

Therefore, the FCC must carefully consider the regulations it promulgates in light of the resulting state consequences.

The clash between the FCC and state governments began with

---

158 Patrick R. Tyson, *The Preemptive Effect of the OSHA Hazard Communication Standard on State and Community Right to Know Laws*, 62 NOTRE DAME L. REV. 1010, 1016-17 (1987) (citing Capital Cities Cable, Inc. v. Crisp, 467 U.S. 691, 699 (1984)).

159 *Louisiana*, 476 U.S. at 374.

160 The Communications Act, in relevant part, states that the FCC was created

> [f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, nationwide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication, and for the purpose of securing a more effective execution of this policy by centralizing authority heretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is hereby created a commission to be known as the "Federal Communications Commission," which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this Act.

The Communications Act of 1934, c.652, I, § 3, 48 Stat. 1064. "Wire communication" is defined as "the transmission of . . . sounds of all kinds by aid of wire, cable, or other like connection . . . including all instrumentalities." 47 U.S.C. § 153(a) (1994).

161 Adu & Dumas, *supra* note 119, at 448. *See Louisiana*, 476 U.S. 355.

162 *Louisiana*, 476 U.S. at 360.

a 1986 United States Supreme Court case, *Louisiana Public Service Commission v. FCC.* [163] *Louisiana* involved an FCC ruling that section 220 of the Communications Act, which expressly directed the FCC to prescribe depreciation practices, pre-empted inconsistent state depreciation regulations for intrastate rate-making purposes to avoid frustration of implementation of federal policies.[164] The FCC argued that a section of the Communications Act explicitly granted the FCC power to prescribe *intrastate* depreciation practices.[165] The Supreme Court stated that the statute may give the FCC authority only over depreciation in the context of *interstate* regulation.[166] The Court rejected the FCC's broad assertion of authority, because it was "at least possible" or "plausible" that the section did not fully support the FCC's contention.[167] The Court also found it significant that Congress did not expressly authorize preemption.[168] Therefore, absent unambiguous statutory language authorizing preemption, the Court preserved state law.[169] Undoubtedly, "the *Louisiana* depreciation decision signaled a shift to greater state hegemony in communications policy."[170]

D. *The FCC's Authority to Preempt State Regulation of Caller ID*

The first step of the *Chevron* test, requiring express congressional intent, is inapplicable to the Caller ID analysis. Congress has not yet passed legislation specifically governing deployment of Caller ID. Instead, after years of inaction regarding the service, the FCC relied upon its general power under the Communications Act to regulate wire communications.[171]

Under the second part of the *Chevron* test, the inquiry is

---

[163] *Id.* at 355; for a discussion of *Louisiana Public Service* and privacy in telecommunications, see generally Adu & Dumas, *supra* note 119.

[164] *Louisiana*, 476 U.S. at 355.

[165] *Id.* at 376.

[166] *Id.* at 377.

[167] *See id.*

[168] *Id.*

[169] *See id.* at 377-78. Following *Louisiana*, the Court of Appeals for the District of Columbia Circuit ruled that "[t]he FCC has the burden . . . of showing with some specificity that [state regulation] would negate the federal policy." National Ass'n of Regulatory Util. v. FCC, 880 F.2d 422, 430 (D.C. Cir. 1989).

[170] DANIEL L. BRENNER, LAW AND REGULATION OF COMMON CARRIERS IN THE COMMUNICATIONS INDUSTRY 67 (1992).

[171] A petition for rulemaking, filed by Joseph Baer, was the impetus for the FCC's campaign to establish a federal model for Caller ID services. Rules and Policies Regarding Calling Number Identification Service—Caller ID, 6 F.C.C.R. 6752, 6753-54 ¶ 7 (1991). The petition proposed a national Caller ID service that offered all customers with unlisted numbers the opportunity to substitute a confidentially registered numeric designation for their billing numbers. *Id.*

"whether the agency's construction of *the statute* is permissible."[172] With respect to the Caller ID analysis, however, no statute besides the Communications Act exists for the FCC to construe. The connection between the broad language of the Communications Act, granting the FCC general authority to regulate wire communications, and the agency's decision to preempt state Caller ID laws is too tenuous. As such, the second branch of the *Chevron* test provides little guidance. Inquiry about whether the regulations that preempt state laws "are arbitrary, capricious, or manifestly contrary to the statute"[173] is useless when the FCC is merely acting under its general power to regulate wire communications. Such an inquiry would enable the FCC to pass almost any regulation, so long as it touched upon wire communications. When the effect of the FCC's rulemaking is to eliminate valued state privacy protections, the Court's presumption in favor of state law necessitates a careful inquiry.[174]

A modified version of the first prong of the *Chevron* test should apply to Caller ID. Even though no federal statute expressly addresses Caller ID, congressional intent regarding regulation of such technology still can, and should, be the appropriate consideration when evaluating the FCC's preemptive regulations regarding the service. Since, Caller ID is part of the converging telecommunication and information industries, a consideration of federal statutes regarding informational privacy in similar industries reveals Congress's intent to protect the public from broad dissemination of personal information.

E. *Convergence and Existing Privacy Protections*

With the proliferation of privacy-invading technologies, Congress has regulated various industries to control the accelerated collection and use of transactional records associated with communications media.[175] As the Department of Commerce ("DoC") recently suggested, however, converging telecommunications services demonstrate "a need for a more comprehensive approach to privacy regulation" across industries.[176] A DoC report on privacy issues recently stated that:

> [t]oday, one set of privacy requirements applies to traditional cable operators; other rules apply to telecommunications com-

---

172 Bergmann, *supra* note 150, at 1214 (emphasis added).
173 *Chevron*, 467 U.S. at 844.
174 *See Louisiana*, 476 U.S. 355.
175 *See* 59 Fed. Reg. 6844.
176 *See id.* 6843.

> mon carriers (with even more specialized rules that apply to the Regional Bell Operating Companies and AT&T); and other firms that provide telecommunications and information services are subject to no restrictions on how they use personal information. Are there any overarching principles that can be extended across specific services in the telecommunications sector? Given the convergence of different industries within this sector, is there a need for a more comprehensive approach to privacy regulation?[177]

Significantly, although the DoC has not yet released a report regarding the responses to this inquiry, it is evidence of the agency's recognition that in the age of the information superhighway, similar privacy concerns of individuals span across different industries within the telecommunications and information sectors.

The Cable Act of 1984[178] and the Video Privacy Protection Act ("Video Act")[179] evidence Congress's intent to provide individuals with informational privacy in this age of the information superhighway's communications media and information services. Caller ID involves identical informational privacy concerns as do the Cable Act and the Video Act. Therefore, a consideration of these laws is useful in determining whether the FCC's ruling regarding call blocking is consistent with what Congress itself would promulgate. Also useful is an analysis of the proposed Telephone Consumer Privacy Protection Act of 1993 ("Consumer Privacy Act")[180] and the recommendations of various informational privacy study commissions.

1. The Cable Television Consumer Protection Act

The subscriber privacy section of the Cable Act restricts Cable providers' abilities to collect and disclose personally identifiable information about an individual.[181] The Cable Act's subscriber privacy section demonstrates Congress's recognition that use of others' personal information must be heavily regulated in order to avoid or diminish privacy intrusions. As the court in *Scofield v. Telecable of Overland Park, Inc.* observed, the privacy requirements were

---

[177] *Id.* 6842-43.

[178] Pub. L. No. 98-549, § 2, 98 Stat. 2794 (codified at 47 U.S.C. § 551 (1988 & Supp. 1993)).

[179] Pub. L. No. 100-618 ¶ 2(a)(1)(2), 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (1988 & Supp. 1993)).

[180] H.R. 3432, 103d Cong., 1st Sess. (1993) [heireinafter Telephone Consumer Privacy Act]. The proposed act directly addresses the issue of Caller ID.

[181] 47 U.S.C. § 551(b), (c). For a general discussion of the privacy protections of the Cable Act, see Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874 (10th Cir. 1992).

included in the Act in response to Congress's observation that " '[c]able systems, particularly those with a "two-way" capability, have an enormous capacity to collect and store personally identifiable information about each cable subscriber. Subscriber records from interactive systems,' Congress noted, 'can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions.' "[182]

The stringent provisions of the Act require that cable operators, at least once each year, provide customers with clear and conspicuous notice of the nature of: 1) personally identifiable information the provider will collect about the subscriber, 2) the uses to which the provider will put the information, 3) the length of time the information will remain on record, 4) the procedures the customer should use to view and correct his or her personal information, and 5) subscriber's rights to enforce the provider's statutory obligations.[183] Additionally, the elaborate provisions of the Act pertaining to collection and disclosure of personally identifiable information[184] evidence Congress's intent to guard individuals' privacy interests. With a few exceptions, cable operators are forbidden from using the cable system to gather or disseminate personally identifiable information about a viewer without prior permission of the individual.[185] A cable viewer may access all personally identifiable information pertaining to the viewer and has

---

182 *Scofield*, 973 F.2d at 876 (citations omitted).

183 The Cable Act, in relevant part, states:

> Protection of subscriber privacy
>
> (a) Notice to subscriber regarding personally identifiable information; "personally identifiable information" defined.
>
> (1) At the time of entering into an agreement to provide any cable service or other service to a subscriber *and at least once a year thereafter*, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of—
>
> (A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;
>
> (B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;
>
> (C) the period during which such information will be maintained by the cable operator;
>
> (D) the times and place at which the subscriber may have access to such information . . . and
>
> (E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber . . . to enforce such limitations.

47 U.S.C. § 551(a) (emphasis added).

184 47 U.S.C. § 551(b), (c).

185 *Id.*

the opportunity to correct any error in the information.[186] Finally, the Cable Act provides that cable operators must destroy personally identifiable information that is no longer necessary for the purpose for which it was collected.[187]

2. The Video Privacy Protection Act of 1988

When Robert Bork was a Supreme Court nominee in 1987, the clerk at a video rental store that Bork patronized released to an inquisitive reporter a list containing the names of films that the judge had rented. Fortunately for Bork, the list contained John Wayne movies, rather than the adult films for which the gossip-hungry reporter obviously had hoped.[188] Congress, outraged by the extraordinarily intrusive behavior, passed the Video Privacy Protection Act of 1988 shortly after this incident.[189] The Act forbids retailers from disclosing video-rental records or other personally identifiable information concerning any consumer.[190]

The Video Act authorizes disclosure of the subject matter of rented videos if the disclosure is solely for the use of marketing goods and services directly to the consumer.[191] On its face, the Video Act may appear to evidence Congress's endorsement of the "traffic in mailing lists that cause us all to be inundated with 'junk mail' of every possible kind."[192] A closer examination of the context in which Congress passed the Video Act, however, manifests that it had no such intent.

Upon realizing how easily anyone could uncover intrusive facts about them, legislators quickly passed the Video Act.[193] Lawmakers were outraged by the Bork incident.[194] At the time that the bill became law, the legislators solely were concerned about protecting themselves from public scrutiny.[195] Had the proposed

---

186 47 U.S.C. § 551(d).
187 47 U.S.C. § 551(e).
188 ROTHFEDER, *supra* note 26, at 27; *see* 59 Fed. Reg. 6844.
189 18 U.S.C. § 2710; *see* 59 Fed. Reg. 6842, 6844.
190 18 U.S.C. § 2710(b).
191 18 U.S.C. § 2710(b)(2)(D)(ii).
192 George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 524 (1990).
193 *See* ROTHFEDER, *supra* note 26, at 27.
194 *Id.*
195 Scott E. Sundby, *"Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1759 (1994); S. REP. No. 599, 100th Cong., 2d Sess. 6 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-41, 4342-45; Dennis McDougal, *Video Rental Privacy Bill Introduced*, L.A. TIMES, Oct. 23, 1987, § 6, at 1 (stating that the Video Act was "the direct result of a Washington weekly newspaper's revelation . . . that Bork and his wife had rented 146 titles from a Washington video outlet during the previous 18 months"); *see* Michael Hinds, *Personal but Not Confidential: A New Debate Over Privacy*, N.Y. TIMES, Feb. 27, 1988, at 56.

bill prohibited use of personal information by telemarketers, the business community surely would have protested the bill. Therefore, the provision allowing use of video rental information for solicitations can best be understood as a compromise that enabled the bill to become law as rapidly as possible.[196] Since the "stated goal of the [Telephone Consumer Protection Act of 1991 was] 'to prohibit certain practices involving the use of telephone equipment for advertising and solicitation purposes,' " it is unlikely that the Video Act indicates Congress's approval of telemarketing solicitations.[197]

3. Telephone Consumer Privacy Protection Act of 1993

The proposed Consumer Privacy Act directly addressed the privacy issues that Caller ID presents.[198] Representative Edward J. Markey sponsored the bill, after noting the need for enhanced privacy protection in this period of "full-fledged technological revolution . . . [that] promises exciting new services and products that will change the way we live, work, and play."[199] Representative Markey, Democrat of Massachusetts and chairman of the House Subcommittee on Telecommunications and Finance, advocated a "privacy bill of rights" by directing the FCC to establish basic privacy protections for *any* telecommunications medium that may infringe on consumer's privacy rights—from interactive television and home shopping to spectrum based technologies, such as cellular phones and personal communications devices.[200] In short, no matter what telecommunications medium consumers use, they must know when personally identifiable information about them is collected. Additionally, those who wish to use or sell personal data must notify consumers, giving individuals the opportunity to curtail such use and abuse of their personal information. According to Representative Markey, the themes of the privacy legislation were "knowledge, notice and no."[201] That is, "[e]veryone should know when information about them is being collected, be told when that information is being sold or rented, and be able to veto that use or

---

196 Indeed, in the subsequent Telephone Consumer Protection Act of 1991, Congress expressly recognized telemarketing as a privacy invader. 47 U.S.C. § 227.

197 James E. Meadows, *The Telephone Consumer Protection Act of 1991: Consumer Salvation or Unconstitutional Restraint?*, COMPUTER LAW., Mar. 1992, at 13.

198 Telephone Consumer Privacy Act, *supra* note 180.

199 139 CONG. REC. E2745 (statement of Rep. Markey).

200 *Id.*; *Privacy Bill of Rights to Target Caller Identification*, ADVANCED INTELLIGENT NETWORK NEWS, Nov. 24, 1993; *see* Ramirez, *supra* note 12, at 10.

201 Larry Tye, *No Private Lives: Proposed 'Bill of Rights' Would Limit Personal Data* (pt. 4), BOSTON GLOBE, Sept. 8, 1993, at 1.

reuse."[202]

Significantly, while generally addressing the issue of integrating and expanding communications networks, the bill specifically focused on the telephone as a privacy invader.[203] Similar to the FCC's regulations, the proposed legislation authorized interstate Caller ID. Importantly, however, the bill provided for a *minimum* standard of per-call blocking.[204] Markey explicitly maintained that states may "enact further privacy protections if they choose," such as per-line blocking.[205]

The proposed Consumer Privacy Act also regulated the use and dissemination of Customer Proprietary Network Information ("CPNI") the telephone company holds about an individual, including name, address, telephone number, and date, destination, and duration of all telephone calls.[206] Many residents and small businesses have no control over use of proprietary data.[207] The proposed bill prohibited the telephone company from disclosing or selling any individual's CPNI without the affirmative consent of the consumer.[208]

Finally, the proposed Consumer Privacy Act recognized that 800 and 900 number services threaten privacy interests, through their use of Automatic Number Identification ("ANI"). These businesses ostensibly use ANI, which provides the caller's directory listing, to verify billing information.[209] Representative Markey,

---

202 *Id.*

203 *See id.*

204 Senator Herbert Kohl, Democrat of Wisconsin, introduced a companion bill to the Senate. Kohl's proposed bill also mandated a minimum safeguard of per-call blocking, but also provided for free per-line blocking for calls made from domestic violence shelters. *Congress Likely to Impose Uniform Caller ID Blocking Rule*, TELEPHONE WK., Feb. 8, 1993; *see Communications: Early Drive Expected on Legislation Held Over From Last Year*, DAILY REP. EXECUTIVES, Jan. 17, 1992, at S33.

205 *See* 139 CONG. REC. E2746 (statement of Rep. Markey).

206 *Id.*; Rules and Policies Regarding Calling Number Identification Service—Caller ID, 9 F.C.C.R. at 1764, 1774 ¶ 61 n.41; 59 Fed. Reg. 6842, 6845. Although the FCC rules regarding CPNI sought to "balance considerations of customer privacy, efficiency, and competitive equity," the mergers, acquisitions and alliances of large local exchange carriers with non-telephone related companies have raised new concerns regarding CPNI use. 9 F.C.C.R. at 1774 ¶ 61. The current rules regulate use of CPNI by the Bell Operating Companies ("BOC's"), which employ CPNI when marketing services and customer premises equipment ("CPE"). The BOC's enhanced service and CPE marketers may use the CPNI data in any way they choose, except if a customer requests otherwise. Current rules require prior authorization for use of CPNI data only for customers with more than 20 telephone lines, since the largest business customers are the ones most likely to require and benefit from the enhanced BOC services and CPE. *See id.*; 139 CONG. REC. E2746 (statement of Rep. Markey); *Privacy Bill of Rights to Target Caller Identification*, *supra* note 200.

207 139 CONG. REC. E2746 (statement of Rep. Markey); *Privacy Bill of Rights to Target Caller Identification*, *supra* note 200.

208 139 CONG. REC. E2746 (statement of Rep. Markey).

209 *See* Seecof, *supra* note 9, at 795.

however, recognized that information gathered from the deployment of ANI "can be recorded, compiled into marketing lists, and then sold to any interested party without any restriction or any requirement to even inform consumers, much less offer the consumers the chance to curtail . . . the practice . . . ."[210] Because "[t]his . . . information is private and should not be marketed and packaged for sale" without the caller's consent, the proposed legislation allowed ANI subscribers to use the information only for billing and collection purposes, or for uses that would facilitate the transaction for which the call was made.[211]

4. Study Commissions on Privacy Issues

a. Committee on Automated Personal Data Systems

Representative Markey was not the first to propose such a sweeping privacy bill of rights. In 1972, the Health, Education, and Welfare Secretary Elliot Richardson formed the Advisory Committee on Automated Personal Data Systems in response to increased use of automated data systems to collect and disseminate personal information about individuals.[212] The Advisory Committee's purpose was to "analyze and make recommendations about the harmful consequences from using automated personal data systems; safeguards that may protect against those consequences; measures that might afford redress; and policy and practices relating to the issuance and use of Social Security numbers."[213] In 1973, the Advisory Committee issued a report[214] in which it recommended principles similar to those in Representative Markey's bill. Congress incorporated some of the Commission's recommendations in the Privacy Act of 1974.[215] The Act, however, was limited to government-held information.[216] Similarly, the Advisory Committee examined "government records and did not focus much attention on the effect of its recommendations on private record keepers."[217]

---

210 139 CONG. REC. E2746-47 (statement of Rep. Markey).

211 *Id.*

212 Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 209 (1993).

213 *Id.*

214 U.S. DEP'T OF HEALTH, EDUCATION, & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS viii (1973); *see* Gellman, *supra* note 212, at 200.

215 Privacy Act of 1974, Pub. L. No. 93-579, § 5(b)(2), 88 Stat. 1906 (1974). Tye, *Proposed 'Bill of Rights' Would Limit Personal Data*, *supra* note 201, at 1. In fact, "[e]ven a cursory review of the Advisory Committee's report and the Privacy Act of 1974 shows a striking similarity in content and organization. Many of the Committee's proposals were enacted almost verbatim in the Privacy Act of 1974." Gellman, *supra* note 212, at 210.

216 Tye; *Proposed 'Bill of Rights' Would Limit Personal Data*, *supra* note 201, at 1.

217 Gellman, *supra* note 212, at 209.

Additionally, it "failed to anticipate technological changes that have made it much easier to gather and collate personal information, and wasn't enforced as vigorously as its sponsors had hoped."[218]

b. Nixon's Domestic Council Committee on the Right to Privacy

Consistent with his belief that "the time has come . . . for a major initiative to define the nature and extent of the basic rights of privacy and to erect new safeguards to ensure that those rights are respected," former president Richard Nixon established the Domestic Council Committee on the Right to Privacy on February 23, 1974.[219] After noting the inadequacies of both Congress's and the Executive Branch's responses to the need for an effective national information policy, the Committee recommended a permanent policy organization within the Executive branch to coordinate a framework for a national information policy.[220] The Committee intended that such an organization would give priority to informational privacy issues.[221]

c. Privacy Protection Study Commission

The Privacy Act of 1974 established the Privacy Protection Study Commission (the "PPSC").[222] Compared to other privacy studies in prior years, the "PPSC had the broadest mandate to review privacy matters in the federal government, state governments, and the private sector."[223] Apparently, concern for individuals' informational privacy was not simply a passing fad limited to governmental abuse of personal information.[224] Instead, the directive to

---

218 Tye, *Proposed 'Bill of Rights' Would Limit Personal Data*, *supra* note 201, at 1.

219 *See* President's 1974 State of the Union Address, 25 WEEKLY COMP. PRES. DOC. 47, 52 (Jan. 30, 1974); Gellman, *supra* note 212, at 212.

220 Gellman, *supra* note 212, at 215.

221 *Id.* at 215.

222 *Id.* at 216; 59 Fed. Reg. 6843; *see* 5 U.S.C. § 552a (1988).

223 Gellman, *supra* note 212, at 216.

224 Originally, people anticipated that "Big Brother—with vast and powerful computers, huge centralized databases, video monitors, and communications equipment at his disposal—would use this technology to entrap individuals and force them into conformity." ROTHFEDER, *supra* note 26, at 22. *See* Trubow, *supra* note 192, at 521. "Every piece of pertinent information would be catalogued and then molded, enhanced, and expunged to suit the needs of Big Brother." ROTHFEDER, *supra* note 26, at 22. Because of the technology explosion, Big Brother never happened. Instead, powerful computers are available to many for a lower price than ever expected. Ironically, although there is no single omniscient Big Brother, anyone who wishes to can play him. As stated by Robert Ellis Smith, editor of the newsletter, *Privacy Journal*, "for very little cost, anybody can learn anything about anybody." *Id.* at 17.

the PPSC to examine privacy concerns in various sectors demonstrated that threats to individual privacy pervaded society.

After examining whether available safeguards adequately protected privacy interests, the PPSC concluded that federal privacy laws must address three policy goals: 1) to balance what an individual must divulge to a record-keeping organization against what the person seeks in return, in order to minimize intrusiveness; 2) to minimize the extent to which recorded information about a person is a basis for any negative decision about the person; and 3) to create reasonable expectations of informational privacy by regulating uses and disclosures of recorded information about an individual.[225] In 1977, the PPSC recommended that Congress develop a privacy bill that embodied many of Representative Markey's suggestions.[226] Unlike the Advisory Committee's recommendations, the study recognized that the United States had become an information society that was under siege by both the private sector and all levels of government.[227]

According to David F. Linowes, chairman of the Privacy Protection Commission, "the recommendations were accepted by members of Congress on both sides of the aisle, and President Carter assured [him] that "he'd convene a Cabinet meeting and urge it to proceed with implementation."[228] Despite enthusiasm for privacy legislation that would implement the recommendations, however, no such bill resulted. Later, Mr. Linowes lamented that "attention always is directed to the crisis of the moment and this never appeared to be a crisis."[229]

Presently, Caller ID and the exploitation of each individual's "computerized alter ego" elevate informational privacy concerns to the forefront of debate, as evidenced by the proposed Telephone Consumer Privacy Protection Act's acceptance of per-line block-

---

225 59 Fed. Reg. 6842.

226 Larry Tye, *supra* note 201, at 1. The Federal Privacy Board's recommendations focused on three objectives to create an effective privacy protection scheme: "to create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return (to minimize intrusiveness); to open up record-keeping operations in ways that will minimize the extent of unfairness in any decision about him made on the basis of it (to maximize fairness); and to create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual (to create legitimate, enforceable expectations of confidentiality)." Gellman, *supra* note 212, at 220; Privacy Protection Study Commission, *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission* (1970).

227 Trubow, *supra* note 192, at 521.

228 Tye, *Proposed 'Bill of Rights' Would Limit Personal Data*, *supra* note 201, at 1.

229 *Id.* Mr. Linowes further noted that today "technology is moving ahead more quickly with communications and superhighways of information, which makes the need for action all the greater." *Id.*

ing.[230] The FCC's decision to banish this valuable privacy protection, however, renders the issue of informational privacy invasion through Caller ID the crisis of the moment, as contemplated by Mr. Linowes.[231]

d. The National Telecommunications and Information Administration's Recognition of Increased Privacy Requirements in the Age of the Information Superhighway

Recently, the Clinton Administration formed the Information Infrastructure Task Force ("IITF") to work with Congress to accelerate the advancement of the National Information Infrastructure ("NII").[232] In its Notice of Inquiry, the IITF stated that since the PPSC's study, technological advances in telecommunications and information technology have occurred.[233] The IITF pursued its goal of protecting privacy interests of individuals while maximizing the flow of information[234] by recently issuing a Notice of Inquiry, in which it stated that "[g]iven the proliferation of computerized data collection and the prospect of converging technologies—computers, telephones and mass media—it is time to reconsider what privacy means in developing electronic communities."[235] The Commission noted that the convergence of technologies may necessitate a more comprehensive approach to privacy protection across different sectors, rather than create the need for a distinct set of principles for telecommunication and information services.[236]

---

230 Law school professor Arthur Miller uses the term "computerized alter ego" when referring to a digital version of each individual's public personae. ROTHFEDER, *supra* note 26, at 16.

231 *Cf.* Tye, *Proposed 'Bill of Rights' Would Limit Personal Data*, *supra* note 201 (indicating that legislators typically devote their efforts towards issues that are crises).

232 The NII refers to the information super highway as "the evolving seamless interactive web of communications networks, computers, data bases, and consumer electronics . . . ." 9 F.C.C.R. at 6842 ¶ 2.

233 *Id.* at 6843.

234 *Id.* at 6842.

235 *Id.* at 6843 ¶ 9.

236 *Id.* at 6842-43 ¶ 7. The Commission lamented that "one set of privacy requirements applies to traditional cable operators; other rules apply to telecommunications common carriers (with even more specialized rules that apply to the Regional Bell Operating Companies and AT&T); and other firms that provide telecommunications and information services are subject to no restrictions on how they use personal information." *Id.* at 6843 ¶ 12. The Commission sought comment by questioning: "[g]iven the convergence of different industries within this sector, is there a need for a more comprehensive approach to privacy regulation? Can 'fair information principles' be extended to interactions between individuals in an electronically wired nation?" *Id.*

F. Implications of Existing Statutes and Previous Study Commissions

Congress has shown its intent to restrict the collection and dissemination of personal information through both the Cable Act and the Video Act. The various study commissions and Representative Markey's proposed Telephone Consumer Privacy Protection Act evidence the urgent need for regulation of the information industry.

The fact that the bill was not enacted should not detract from the significance of legislation that seeks to preserve per-line blocking. As illuminated in the responses to the FCC's notice on proposed rulemaking,[237] fierce opposition to Caller ID blocking mechanisms exists. Because Representative Markey's bill leaves open the possibility of per-line blocking on a state-by-state basis, it provokes strong opposition. Indeed, regional holding companies voiced their concern that per-line blocking would eliminate the utility of the Caller ID service by making it too easy for individuals to block calls. Additionally, it is difficult to pass legislation when the business community vehemently opposes it.[238]

Overall, Congress has consistently illustrated its intent to restrict collection and dissemination of individuals' personal information gathered from transactional records associated with communications media and information services. Most significantly, the Cable Act imposes upon cable operators extraordinarily stringent requirements providing that consumers must have notice and the opportunity to consent to the collection and use of personally identifiable information. The Video Act also manifests Congress's concern about unrestricted use of personal information, given that personal facts "may be of such a highly sensitive and personal nature that, although correct, they are potentially harmful and embarrassing if disseminated carelessly."[239] Since Caller ID is also a telecommunications service of the information superhighway, the FCC's decision to promulgate regulations that diminish individuals' state privacy protections must not conflict with the congressional intent to protect informational privacy, evidenced in

---

237 6 F.C.C.R. at 6752.

238 *Cf.* Gellman, *supra* note 212, at 237 (describing the difficulty with creating a federal data protection agency in the face of opposition from the business community). Businesses value Caller ID because it facilitates customer service by taking 20-30 seconds off of each call that matches a database record. Grigonis, *supra* note 44, at 57. Additionally, the value of Caller ID to the telemarketing industry ensures opposition to Representative Markey's proposal to allow per-line blocking.

239 Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. Rev. 133, 133 (1991).

other statutes addressing telecommunications and information industries.[240] Accordingly, the FCC should allow states to continue to protect their citizens' privacy by offering per-line blocking.[241]

CONCLUSION

In the past few decades, informational privacy has been a concern to both the legislative and executive branches. Thus far, the horror stories about privacy invasions that the popular press publicizes have led to legislation in various telecommunications sectors rather than a single, expansive law covering all telecommunications industries. Nonetheless, because these industries are converging and similar privacy concerns exist in each, it is appropriate to examine legislation that protects privacy in other telecommunications mediums in order to discern congressional intent regarding the Caller ID service.

The FCC's decision to require per-call blocking is a valid and necessary decision within those states that do not offer any blocking mechanisms. Congress has not expressly stated its intent regarding the merits of per-line and per-call blocking. Nonetheless, a consideration of the other statutes regarding privacy with respect to telecommunications-generated information indicates that Congress would not approve Caller ID without per-call blocking, which is the minimum privacy protection available. Therefore, to the extent that the FCC's ruling preempts state laws that offer no privacy protection, the regulations are consistent with Congress's intent.

The FCC can not preempt state regulation of Caller ID by eliminating per-line blocking, since this would conflict with Congress's intent to increase individuals' control over the collection and use of their personal information. Although Congress has not formally resolved the issue of the Caller ID privacy debate regarding the merits of per-line blocking, various statutes evidence Congress's intent to "ensure the perpetuation of . . . privacy rights as communications and computer technology continue to merge and evolve."[242] Additionally, the establishment of various study commissions in the last few decades and their recommendations evidence the long-standing significance of personal informational privacy issues.

Although the Communications Act authorizes the Agency to regulate Caller ID as a service of wire communications, the FCC's

---

[240] *See Louisiana*, 476 U.S. 355.
[241] *See* 9 F.C.C.R. at 1775-76 ¶ 69.
[242] *See* Telephone Consumer Privacy Act, *supra* note 180.

regulations, after seven years of silence, preempt state privacy protections in contravention of Congress's intent. For now, per-line blocking may be the only way to resolve the conflict between callers and called parties. The FCC exceeded its authority by banning this much-needed option upon which many citizens rely to protect themselves.

Even if the FCC abandons its ruling and allows states to retain per-call blocking, "the current applications of the Caller ID technology represent only the tip of the iceberg of privacy issues that will be implicated by the growing demand for exchange of customer identification information as the NII develops."[243] As technological innovation in electronic media and telecommunications industries continues, greater privacy concerns will evolve. Since it will likely be impossible for Congress to keep pace with sophisticated, new technological advancements, it must pass cohesive legislation that will guard privacy in all information industries, both now and in the future. "If dealt with on a piecemeal basis, the inconsistencies in treatment of these developments and the problems they create are likely to be exacerbated."[244] Finally, Congress must clearly mandate that the FCC enforce such legislation with a presumption in favor of informational privacy protection, so that the Commission never again will err as it did in abolishing per-line blocking.

*Laura V. Eng**

---

243 Richard E. Wiley & Robert J. Butler, *National Information Infrastructure: Preserving Personal Space in Cyberspace*, COMM. LAW., Fall 1994, at 27.

244 *Id.*

* Jodi-Lynne Bayrd and Shai Waisman provided valuable editorial comments on earlier versions of this work. My thanks to Daniel Goldfisher for his inspiration and assistance in this article's development. I am grateful to Adrian Spratt, Assistant Attorney General, New York State, for his guidance in this and many other endeavors.