CALLER ID AND FAIR CREDIT REPORTING: TECHNOLOGY AND TRADITIONAL NOTIONS OF PRIVACY CLASH

*Honorable Matthew J. Rinaldo**

I. Introduction

In a 1990 national opinion poll, seventy-nine percent of those surveyed expressed concern about threats to their privacy.[1] While locked doors and drawn shades traditionally have provided Americans with sufficient privacy, they are of little use in today's technological revolution. Telephones, credit reports, and computers have broken down the walls of personal privacy to an astonishing degree in a short period of time. As the House Energy and Commerce Committee's Ranking Republican Member on the Subcommittee on Telecommunications and Finance, I am particularly attuned to, and active in, the legislative debate over American consumers' concerns about threats to their privacy. I am committed to protecting the reasonable expectation of privacy, while balancing those rights with the numerous economic benefits that come with the telecommunications revolution.

Two examples of this clash between consumer privacy and technological innovation involve telephone number identification technology (or so-called "Caller ID") and credit reports. Caller ID has thrust New Jersey into the forefront of this debate.

---

* United States Congressman, 7th Congressional District of New Jersey. B.S., Rutgers (1953); M.B.A., Seton Hall University (1959); Ph.D., New York University School of Public Administration (1979). Mr. Rinaldo (R-Union, New Jersey) was born on September 1, 1931 in Elizabeth, New Jersey. In 1963, he was elected as president of the Union Township Zoning Board and later that year became a Union County Freeholder. Mr. Rinaldo served in the New Jersey Senate for five years after being elected in 1967 and re-elected in 1971. Mr. Rinaldo was elected in 1972 to serve New Jersey's 7th Congressional District. In Congress, Mr. Rinaldo is a member of the Committee on Energy and Commerce where he serves as the ranking minority member of the Subcommittee on Telecommunications and Finance. He also serves on the Select Committee on Aging.

[1] THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE, at v (1990) (a national opinion survey conducted for Equifax, Inc., by Louis Harris & Associates and Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University).

In the summer of 1987, New Jersey Bell became the first company to seek permission to provide Caller ID service to its customers.[2] This service displays the telephone number of the calling party on a display screen attached to the telephone of the party receiving the call. It allows the latter to ascertain the caller's phone number.[3] Caller ID has certain undeniable social benefits; specifically, it has significantly reduced the number of requests to New Jersey Bell to trace obscene, annoying or harassing telephone callers.[4] Rather than involving New Jersey Bell to trace these annoying calls, consumers with Caller ID may simply choose to confront the caller with the fact that they know the caller's number, thus taking away the anonymity that such callers hide behind.[5]

Computerized credit reports also have generated numerous privacy complaints. The three major credit reporting agencies have discovered that selling credit information about their customers is extremely profitable.[6] As a result, individual credit his-

---

2 On July 16, 1987, New Jersey Bell requested permission from the New Jersey Board of Public Utilities (BPU) to provide "Caller Identification" service on a limited basis. Filing by New Jersey Bell Tel. Co. of a Revision of Tariff B.P.U.-N.J. No. 2, Providing for the Introduction of CLASS Calling Service on a Limited Basis, Docket No. TT87070560 (N.J. Bd. of Pub. Utils. July 16, 1987). For a historical account of New Jersey Bell's quest for state approval of Caller ID services see Glenn Chatmas 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, 145-52 (1989) [hereinafter Smith, *Caller Identification*].

3 *See* Smith, *Caller Identification*, *supra* note 2, at 145. *See also*, Calvin Sims, *Harassing Calls Show Decline When Phones Identify Callers*, NEW YORK TIMES, Aug. 5, 1989, at A1 [hereinafter Sims, *Harassing Calls*]. The New Jersey Bell system allows users to attach a small screen to the telephone which will display the caller's number. This technology also allows the telephone company to make a computer record of where and when harassing calls originated. The customer merely has to dial a code when the call is made. Sims, *Harassing Calls*, at A1.

4 In its first test of Caller Identification, New Jersey Bell reported that there was a 49 percent decrease in requests from customers for it to trace calls. *See* Sims, *Harassing Calls*, *supra* note 3, at A1.

5 As a matter of fact, the telephone companies encourage customers to confront persons who harass them by making obscene or unwanted telephone calls. In marketing Caller Identification service, some telephone companies are airing television commercials which depict such a situation. Critics, however, argue that such a practice could be dangerous and may lead to vigilantism. *Caller-Id Technology: Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. 111 (1990)(testimony of Dr. Mark N. Cooper, Director of Research, Consumer Federation of America).

6 Business Week reports that $2 billion was to be spent in 1989 by companies

tories are being used in marketing, developing mailing lists, and a variety of other sales activities.[7] In most cases, the individual is unaware that his or her financial records are being sold to third parties.[8] The widespread availability of such credit data seriously compromises the privacy of millions of consumers.

This article initially explains the technology that makes both Caller ID and computer-generated credit reports possible and outlines their current commercial availability. It also examines how this technology impinges upon consumers' reasonable expectation and concomitant legal claim to privacy. The article concludes with an examination of legislative proposals that address consumers' privacy concerns without unnecessarily impeding the innovation and growth of these dynamic technologies.

II. Caller ID

A. *The Technology That Makes Caller ID Possible*

New Jersey Bell and other telephone companies are cur-

---

trying to find the right customers to make a sales pitch to or offer credit. Jeffery Rothfeder, et al., *Is Nothing Private?*, BUS. WK., Sept. 4, 1989, at 74-76 [hereinafter Rothfeder, *Is Nothing Private?*]. Credit histories are compiled by three companies, TRW of Orange, California, Equifax of Atlanta, Georgia and Trans Union Credit Information of Chicago, Illinois. These companies reported revenues for 1988 were $335 million, $259 million and $300 million respectively. *Id.* at 81. These companies have 400 million records on 160 million individuals. Such records are compiled and sold in lists broken down by sex, age and income. *Id.* For example, the data can be manipulated to find the names of Hispanics "who earn $500,000 a year and have $10,00 available on their credit cards." *Id.* at 76. *See also Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 222 (1991)(prepared Testimony of Dr. Mary J. Culnan, Associate Professor, Georgetown University School of Business Administration).

7 TRW, one of the three largest credit bureaus, in a booklet discusses its marketing database as:

> [b]eing built by blending hundreds of individuals demographic and financial information pieces. Each of these bits of information help to define a person's gender, age, marital status, financial lifestyle, etc. . . . A model statistically defines individuals based upon the hundreds of pieces of information contained in the database.

Amendments to the Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs, 101st Cong., 2d Sess. 650 (1990)(TRW booklet entitled "The Perfect Match").

8 A Business Week editor, through his personal computer, was able to gain access to Vice President Dan Quayle's credit history by paying a $500 initial fee. While the editor was in the database he was able to check credit reports of his colleagues for about $15 a report. Rothfeder, *Is Nothing Private?*, *supra* note 6, at 74.

rently in the process of replacing their switching technology, by which they route calls, from a central location, throughout a telephone company's network. A new technology known as Signalling System Seven, or SS7, is being deployed throughout the network. SS7 has significantly enhanced the speed and type of information traveling through the network in providing both local and long distance telephone service.

In addition, SS7 has permitted New Jersey Bell to offer a host of new services known as Custom Local Area Switching Services, or CLASS. These new, sophisticated services rely on SS7's switching technology to provide more than just voice transmission, including features such as Caller ID and other so-called "smart services."[9] With Caller ID, a subscriber to the service must also purchase or lease a small display screen for his or her telephone. When someone calls the subscriber, the calling party's telephone number appears on the display.[10] The number appears while the telephone is ringing, and some models have a memory bank that may retain the numbers of as many as the last one-hundred callers.

B. *Commercial Availability*

Caller ID is currently being offered on a trial or permanent basis in twenty-two states.[11] For example, New Jersey Bell has offered Caller ID in New Jersey since October 1988.[12] However, in other states, Caller ID has yet to clear some legal and regulatory hurdles. The Pennsylvania Supreme Court has prohibited

---

9 One such smart service is "return call," which allows the called party to return an unanswered call without knowing the calling party's number by simply pressing several numbers.

10 *See* Smith, *Caller Identification*, *supra* note 2, at 145.

11 Anthony Ramirez, *New York State Approves Caller-Identification Service*, NEW YORK TIMES, Mar. 12, 1992, at D1 [hereinafter Ramirez, *New York Approves Caller-Identification*].

12 On October 20, 1988 the New Jersey BPU issued an order approving statewide implementation of Caller Identification technology over a four year period. New Jersey Bd. of Pub. Utils., Filing by N.J. Bell Tel. Co. of a Revision of Tariff B.P.U.-N.J. No. 2, Providing for Approval of Provision of CLASS Calling Service Tariff Basis and the Withdrawal of Interim Limited CLASS Calling Service Tariff, Docket No. TT88070825 (N.J. Bd. of Pub. Utils. Oct. 20, 1988). Christine Todd Whitman, then President of the New Jersey BPU, dissented from the order citing privacy concerns. *See* Smith, *Caller Identification*, *supra* note 2, at 146 n.2, 151-52.

Caller ID on the grounds that it violates the state's wiretap law.[13] New York's Public Service Commission recently approved caller identification service with the condition that the telephone company offer call blocking.[14]

C. *Privacy as a Constitutional Right*

Given that Caller ID seems to be a useful, socially beneficial service, one might logically ask: What is the privacy problem? It certainly does not lie with the obscene or harassing caller; that

---

[13] Barasch v. Bell Tel. Co. of Pa., No. J - 190-1991, Slip op. at 9 (Pa. Mar. 18, 1992). On November 9, 1989, the Pennsylvania Public Utility Commission approved a tariff filed by Bell of Pennsylvania to provide Caller Identification service. Barasch v. Pennsylvania Pub. Util. Comm'n, 575 A.2d 79, 83 (Pa. Commw. Ct. 1990). The Commission found that Caller ID can save lives, "annoying, harassing, abusive, obscene and terroristic telephone calls can be curtailed; false bomb threats to public schools, false fire alarms and other harassing and life threatening prank calls may be eliminated or reduced." *Id.* at 82.

An appeal was filed which alleged that Caller ID without a blocking device violated Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Stat. Ann. §§ 5701-5781 (1983). The appellants also argued that Call ID violated privacy rights protected by the state constitution. The Pennsylvania Commonwealth Court held that the Caller ID was illegal because it violated the wire tap statute's general prohibition against unilateral "trap and trace" devices. *Barasch*, 576 A.2d at 85. Such trap and trace devices which are illegal "capture[] the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 Pa. Stat. Ann. § 5702. The court then discussed the privacy arguments by first finding that the state and federal constitution applies to Pennsylvania Bell through the doctrine of state action. *Id.* at 86-88. For an interesting discussion of the state action doctrine as applied to telephone companies in Caller Identification cases see Smith, *Caller Identification*, *supra* note 2, at 152-67. The court then held that Caller ID, without a blocking device, violates the "privacy rights of the people." *Barasch*, 576 A.2d at 89. Therefore, "consumers of telephone service should not suffer an invasion, erosion or deprivation of their privacy rights to protect the unascertainable number of individuals or groups who receive nuisance, obscene or annoying telephone calls which can already be traced or otherwise dealt with by existing services provided by Bell." *Id.* See Laura Holt Jones, Note, *Informational Privacy and Property Rights: Caller*ID and the Barasch Court*, 13 Geo. Mason U.L. Rev. 447 (1990) for a detailed review of the *Barasch* Commonwealth Court decision and an overview of the emerging constitutional doctrine of informational privacy.

The Pennsylvania Supreme Court affirmed the appeals court decision on the grounds that Caller ID violates the "trap and trace" prohibitions of the Wire Tap Act. Barasch v. Bell Tel. Co. of Pa., No. J. - 190-1991, Slip op. at 9 (Pa. Mar. 18, 1992). The court did not reach the constitutional privacy issue because "courts should not decide constitutional issues in cases which can properly be decided on non-constitutional grounds." *Barasch*, Slip op. at 16.

[14] *See* Ramirez, *New York Approves Caller-Identification*, *supra* note 11, at D1 & D17.

caller arguably waives his or her right to privacy once the law has been broken by making an obscene or harassing call.[15] Instead, the privacy concern lies with those consumers who do not want their number revealed. This is likely to apply to subscribers with unlisted numbers. Caller ID, offered on an unrestricted basis, would release those unlisted numbers to the called party. In addition, Caller ID also presents a whole host of other problems for consumers since businesses increasingly are frequent customers of the technology. By using Caller ID, in conjunction with their own data bases, businesses may instantly obtain important billing information (name, address, and past transaction and account information) which speeds the completion of telemarketing business transactions.[16] This is a legitimate, unobjectionable use of the technology. Unfortunately, some businesses, in turn, sell that information to other telemarketing firms, which may then invade the privacy of individuals through repeated, undesired, and invasive calls to their homes.[17]

While not explicitly provided for in the Constitution, the Supreme Court has recognized a constitutional right to privacy.[18]

---

15 For example, in New Jersey it is illegal to make anonymous phone calls using "offensively coarse language, or any other manner likely to cause annoyance or alarm." N.J. STAT. ANN. § 2C:33-4(a) (1981 & Supp. 1991).

16 American Express uses such technology in transacting business by phone with its customers. American Express, however, found that making its customers aware of this practice was bad business.

> As the phone was ringing, the company would match the incoming phone number with the appropriate customer file, and answer the phone by greeting the customer by name. American Express stopped greeting customers by name after people objected to the practice, but they continue to use the technology to call up customer files.

Telemarketing/Privacy Issues: Hearing Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce, 102d Cong., 1st Sess. 50 (1991)(testimony of Janlori Goldman, Legislative Counsel, American Civil Liberties Union (ACLU)).

17 The Wall Street Journal recently asked if a phone company should have the right to release phone numbers, especially unlisted ones, to individuals and institutions willing to pay a fee for the information. "[W]ith this new technology-and some good data banks-[a company] could match a person's phone number with the story of his life." Mary Lu Carnevale, *Making a Phone Call Might Mean Telling The World About You*, WALL STREET J., Nov. 28, 1989, at A8.

18 *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965)(right to marital privacy was found in the "penumbras" of the First, Third, Fourth, Fifth and Ninth Amendments); Eisenstadt v. Baird, 405 U.S. 438 (1972)(right to privacy protects unmarried from using contraceptives); Roe v. Wade, 410 U.S. 113 (1973)(a woman's right to privacy prevents the state from regulation of abortion during the first trimester).

These cases arguably emanated, in part, from the seminal tract of future-Supreme Court Justice Brandeis. In 1890, Louis Brandeis and Samuel Warren wrote that "[i]n every case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent."[19] Justice Brandeis later interpreted this right to privacy broadly, including recognizing a specific privacy right — "the right to be left alone."[20]

The Court confirmed the existence of this right to privacy in two important cases. First, in *Katz v. United States*, the Court held that there are zones of privacy in which a person had a reasonable expectation of privacy.[21] Interpreting the Fourth Amendment's prohibition against "unreasonable search and seizures," the Court held in *Katz* that people were protected from warrantless electronic surveillance of their telephone calls by other parties. Justice Harlan, in his famous *Katz* concurrence, provided that in order to find a privacy right "a person must have exhibited an actual (subjective) expectation of privacy and . . . that the expectation be one that society is prepared to recognize as 'reasonable.' "[22] In 1979, the Court noted in *Whalen v. Roe* that the right to privacy may entitle individuals to control the dissemination of personal information about themselves.[23] Justice Stevens, writing for the Court, found that there are two types of rights to privacy.[24] First, there is the "individual['s] interest in avoiding disclosure of personal matters and another is the interest in independence in making certain kinds of important decisions."[25]

---

19 Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193, 199 (1890).

20 Olmstead v. United States, 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting). In *Olmstead*, a divided court held that a wiretap did not violate the Fourth Amendment because such action did not literally constitute a search and seizure. The Court rejected this literal reading of the Fourth Amendment in Katz v. United States, 389 U.S. 346, 353 (1967), where the Court held that "[t]he government's activities in electronically listening to and recording petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth . . ."

21 389 U.S. at 351-52.

22 *Id.* at 361 (Harlan, J., concurring).

23 429 U.S. 589 (1977). In *Whalen*, the Court upheld a New York statute which required doctors to disclose patients names and addresses who were taking certain prescribed medication. This information was, in turn, placed in a computer database in order to avoid the misuse of drugs. *Id.* at 591-92.

24 *Id.* at 599.

25 *Id.* at 599-600 (footnotes omitted).

Although the *Whalen* Court did not strike the New York statute since there was sufficient safeguards to protect privacy, this opinion serves as judicial recognition of an informational privacy right.[26] Such an informational privacy right has been recognized explicitly by six circuit courts.[27]

The Court, however, has been reluctant to extend the right of privacy to protect telephone numbers that are dialed and the person dialing them. Basing its decision on the reasonable expectation of privacy articulated in *Katz*, the Court found in *Smith v. Maryland*,[28] that individuals do not expect the numbers they dial to be private. The Court based its reasoning largely on an historical perspective of how telephone calls were made. The Court noted that prior to the use of mechanical and electronic switches in the network, live operators connected calls, thus abrogating any reasonable expectation of privacy.[29] The Court apparently believed that the caller's expectation did not change with the advent of new technology that ended the use of live operators.[30]

D. *The Legality of Caller ID*

Congress strongly disagreed with the *Smith* Court's conclusion. In response to the Court's reluctance to extend the right to privacy to dialed numbers, Congress passed the Electronic Communications Privacy Act of 1986 (ECPA).[31] This Act extended telephone customer protections in the Wiretap Act of 1968[32] explicitly to include dialed numbers along with the actual content

---

[26] Justice Brennan, in a concurring opinion, stated that "[b]road dissemination by state officials of such information [names, addresses and prescription information] would clearly implicate constitutional protected privacy rights, and would presumably be justified only by a compelling state interests." *Id.* at 606 (Brennan, J., concurring)(citing Roe v. Wade, 410 U.S. 113, 155-56 (1973)).

[27] *See* Smith, *Caller Identification*, *supra* note 2, at 175 nn.143-48 and accompanying text.

[28] 442 U.S. 735, 744 (1979).

[29] *Id.*

[30] In *Smith v. Maryland*, the police requested that the telephone company install a "pen register" at its central location to record telephone numbers dialed from a suspect's home. *Id.* at 737.

[31] P.L. 99-508, 100 Stat. 1848, 18 U.S.C. § 2511 (1988).

[32] The Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510-2521 (1988).

of the telephone call.[33]

Whether or not Caller ID is legal under ECPA seems unclear because Caller ID was not specifically addressed in ECPA. Analysis by the Congressional Research Service and the American Civil Liberties Union suggests that Caller ID could be illegal under the ECPA.[34] Recently, the ACLU testified before Congress that:

> As drafted, ECPA contemplates the use of trap and trace devices [of which Caller ID is one] by only two parties — law enforcement, which must first obtain a court order, and telephone service providers, which must meet one of three exceptions. All other uses are prohibited.
>
> Caller ID devices squarely fit the law's definition of a trap and device that 'captures' and identifies 'the originating number . . . from which a wire or electronic communication was transmitted. ECPA prohibits the use of a trap and trace device without court order unless one of three exceptions are met. The three exceptions only apply to 'providers' of telephone services. Thus it appears that the use of a trap and trace device by a telephone *subscriber* is prohibited.[35]

E. *Privacy and Caller ID*

In order to address the privacy concerns of calling parties inherent in Caller ID, the House Energy and Commerce Committee's Telecommunications Subcommittee recently approved legislation to mandate a minimum level of protection for calling parties.[36] The bill the subcommittee approved attempts to balance the privacy concerns of the calling party and the called party by mandating that, at a minimum, the states must allow all callers

---

[33] The Senate report which accompanied ECPA specifically articulated that the use of a pen register without a court order is illegal. S. REP. No. 541, 99th Cong., 2d Sess. 45-46, *reprinted in* 1986 U.S.C.C.A.N 3599-3600.

[34] *Telephone Privacy Act of 1990: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Administration of Justice of the House Judiciary Comm.*, 101st Cong., 2d Sess. 115-17 (1990) (prepared statement of Janlori Goldman, Legislative Counsel, ACLU).

[35] *Id.* at 117-18 (quoting 18 U.S.C. § 3127(4)(emphasis in original)).

[36] H.R. 1305, 102d Cong., 1st Sess. (1991). (the full text of H.R. 1305 is set out in the appendix to this article). See H.R. REP. 324, 102d Cong., 1st Sess. 9-15 (1991) for a section-by-section analysis of H.R. 1305. H.R. 1305 was approved on June 20, 1991 by the Subcommittee on Telecommunications and Finance. The Energy and Commerce Committee subsequently reported H.R. 1305 out by a voice vote on July 30, 1991 with amendments.

to block, on a "per call" basis, the transmission of their telephone numbers.[37] States would be free to adopt a more restrictive policy (such as allowing a total block of *all* calls from a certain number — known as "per line" blocking — provided the policy does not render Caller ID service useless).[38] As a main proponent and chief sponsor of this legislative initiative, I have attempted to balance the calling party's right to privacy with the called party's right to privacy in terms of Caller ID's effect.[39]

Additionally, one fact worthy of note is that both the calling and called party share, at various times, the same perspective — depending on whether we are calling someone or being called. As the ACLU testified, "each party, at different times and for different reasons, has an interest in receiving phone numbers and in limiting dissemination of their numbers."[40] The goal of federal legislation is to construct rules that meet the reasonable expectations of parties whether calling or being called.

1. The Calling Party

It has been argued that Caller ID does not invade the privacy

---

[37] H.R. 1305 at § 3(b). Unrestricted Caller ID is not necessary.

> In arguing for Caller ID without blocking, proponents of such regulatory policy point to the need of consumers to obtain the number of the obscene or harassing caller. Yet once a subscriber obtains that number, he or she will probably choose to take one of three options: call the police; call back the harassing caller and confront that person; or do nothing at all. Calling the police is just as easily and effectively done by Using Call Trace. To confront the harassing caller, Call Return does the job.

H.R. REP. 324 at 11-12.

Call Trace is a device which allows the victim of a harassing phone calls to automatically trace a number and have it saved in the telephone company's switch for use by law enforcement authorities. The victim can activate Call Trace by dialing a code after the victim hangs up the phone. *Id.* at 11. In a documented case in Essex County, New Jersey, the police apprehended a suspected child molester by using a call tracing system. The suspect called a police desk asking why the police were looking for him. The caller claimed he was at home and when the call was traced, the system refuted this assertion. The police apprehended the suspect at a convenience store. Robert Asa Crook, *Sorry, Wrong Number: The Effect of Telephone Technology on Privacy Rights*, 26 WAKE FOREST L. REV. 670 n.11 (1991)(citing *Look Who's Calling*, THE L.A. DAILY J., Oct. 5, 1989, at 6.)

[38] H.R. REP., *supra* note 37, 324 at 6-8.

[39] *Id.* at 10.

[40] *Hearing Before the Subcomm. on Courts, Intellectual Property, and the Administration of Justice of the House Judiciary Comm.*, 101st Cong., 2d Sess. 123 (1990)(statement of Janlori Goldman, Legislative Counsel, ACLU).

of the calling party as it only releases the telephone number, an "impersonal" piece of information that callers do not really care about having revealed.[41] This ignores the fact that cross directories — which allow one to look up the name and address associated with a telephone number — can easily transform this "impersonal" information allowing a person to identify, with great specificity, the person and place of residence of the calling party.[42] Additionally, Caller ID releases the information in a manner which gives more information than can be found in the telephone listings.[43] For example, if one called local stores to

---

41 James E. Katz, *Caller-ID, Privacy and Social Processes*, TELECOMMUNICATIONS POLICY, Oct. 1990, at 380.

42 *Id.* at 380. Katz argues that Caller ID does nothing to erode the privacy of the caller. He relies on customs and traditions before the advent of Caller ID. Such customs, he argues, are that all callers would identify themselves to the calling party when making a call. *Id.* at 377 (citing ELIZABETH POST, EMILY POST'S ETIQUETTE 165-67 (14th ed. 1984)). *See also* Smith, *Caller Identification*, *supra* note 2, at 149.

43 *Id.* at 183-85. The courts have declined to allow the release of "impersonal" information that can be reasonably used to identify individuals. In Thornburgh v. American College of Obstetricians, the Supreme Court invalidated an abortion notification statute. 476 U.S. 747, 766-67 (1986). The Court reasoned that even though the statute did not require the reporting of the woman's name, "the amount of information about her and the circumstances under which she had an abortion are so detailed that identification is likely." *Id.* "Identification is the obvious purpose of these extreme reporting requirements." *Id.* at 767.

Justice Scalia recognized the possibility of an informational privacy right when he sat on the United States Court of Appeals for the D.C. Circuit. In Arieff v. United States Dep't of the Navy, a journalist made a Freedom of Information Request (FOIA) for documents which disclosed the name and amounts of prescription drugs provided to doctors who served former members of Congress and Supreme Court Justices. 712 F.2d 1462, 1465 (D.C. Cir. 1983). Such information did not identify any one user of drugs. Scalia asked whether under the circumstances such information could lead *indirectly* to the medical conditions of the persons using the drugs. *Id.* at 1468. As Smith states in his insightful article on Caller ID:

> The *Arieff* approach—which, as with the Supreme Court's approach in *Thornburgh*, elevates the substance of a privacy invasion over its form—seems at least as well suited to the informational privacy context. It makes little difference whether the harms the informational privacy right seeks to avoid are caused by the information per se or by the information *in the context in which it is received*. The policies behind the right are threatened in either situation.

Smith, *Caller Identification*, *supra* note 2, at 185 (footnote omitted) (emphasis in original).

Justice Stewart in his dissent to Smith v. Maryland recognized that telephone numbers are not "impersonal information."

> The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself, are not without content. Most private telephone subscribers . . . [would not] be happy to have broadcast

compare prices, then one's number is identified as belonging to someone wanting to purchase a particular item. This is valuable information for a retailer, and it should be entitled to some caller privacy protection.

Caller ID's relation to the calling party's right to privacy can best be assessed by examining three aspects of that right: 1) the expectation of privacy that the calling party has, 2) the control the calling party has over disseminating his or her telephone number, and 3) the potential impact that the release of the telephone number would have. I believe Caller ID infringes on the calling party's reasonable "expectation of privacy"[44] in protecting the person's telephone number. In enacting ECPA, Congress codified protection of this expectation of privacy that calling parties had arguably expected since live operators were replaced by switches in the telephone network.[45]

Among telephone callers, those who have unlisted telephone numbers[46] would seem to have a heightened privacy expectation. One may reasonably argue that they do not expect that their telephone numbers will be revealed to the public. On this basis, Caller ID poses the threat of undermining a service (an unlisted telephone number) for which the subscriber pays a monthly fee. Some believe it is unconscionable for the telephone company to offer a service for a fee, like Caller ID on an unrestricted basis, that could eviscerate the utility of another service, such as an unlisted number, for which a subscriber also pays a fee.

Another aspect of the right to privacy is the "right to infor-

---

> to the world a list of the local or long distance numbers they have called. This not because such a list might be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the more intimate details of a person's life.

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

[44] *See* Katz v. United States, 389 U.S. 347, 361 (1967)(Harlan, J., concurring). The Supreme Court has not addressed the issue of privacy and Caller ID. However, in cases where the Court did focus on the disclosure of information it looked to see how that disclosure impacted on other substantive rights. *See, e.g.*, NAACP v. Alabama, 424 U.S. 693 (1976)(based on the First Amendment, the Court prevented Alabama from requiring the NAACP to disclose its membership list).

[45] *See* S. REP. No. 541, 99th Cong., 2d Sess. 10, *reprinted in* 1986 U.S.C.C.A.N. 3564.

[46] In New Jersey, for example, nearly 40% of the telephone subscribers have unlisted numbers.

mational privacy."[47] That is, a person possesses the right to choose when to disclose information about himself or herself. Traditionally, the calling party always chose whether to disclose his or her telephone number. Caller ID offered on an unrestricted basis reverses the status quo, for it would reveal the calling party's number regardless of the caller's wishes. Many believe that a person should not have to give up his or her phone number as a condition for using the telephone.[48]

The potential negative impact of Caller ID on the privacy rights and non-disclosure interests of the calling party includes the threat of disclosure of compromising personal information and the possibility of harassment. Specifically, Caller ID can lead to violations of the right of an individual to avoid the disclosure of information "which could lead to embarrassment, stigmatization, or other reputational injury."[49] For example, if an AIDS hotline used Caller ID to identify callers and then released that information, the calling parties might be identified in their communities and then subject to discriminatory behavior.[50]

Besides the danger of discrimination against those who call a public service number, such as a health crisis line, Caller ID can affect those who are calling to give information.[51] Anonymous whistle-blowers, people with "tips" for the police, and union organizers may all be put at risk by Caller ID. With such individuals in mind, the Supreme Court has supported anonymity not only on right to privacy grounds, but also because this right safeguards other freedoms, such as freedom of speech and association.[52]

---

47 Smith, *Caller Identification*, *supra* note 2, at 177. "Unlike the fourth amendment, the informational privacy right transcends barriers against initial acquisition of information to provide protection against its subsequent disclosure." *Id.*

48 *See generally, Telemarketing/Privacy Issues: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce*, 102d Cong., 1st Sess. 45-52 (1991)(statement of Janlori Goldman, Legislative Counsel, ACLU).

49 Smith, *Caller Identification*, *supra* note 2, at 188. *See also* Comment, *Conceptualizing National Identification: Informational Privacy Rights Protected*, 19 J. MARSHALL L. REV. 1007, 1014-15 (1986)(provides a list of injuries resulting from unwarranted collection and disclosure of personal information).

50 H.R. REP. 324, *supra* note 36, at 5.

51 Robert Asa Crook, *Sorry, Wrong Number: The Effect of Telephone Technology on Privacy Rights*, 26 WAKE FOREST L. REV. 669, 672 (1991); Sims, *Harassing Calls*, *supra* note 3, at 35.

52 *See, e.g.*, Lamont v. Postmaster General, 381 U.S. 301 (1964)(struck require-

While only a small number of Caller ID applications would implicate the privacy right of the calling party to avoid stigmatization, a potentially larger number of uses of Caller ID — such as in private homes — can lead to violations of the calling party's "right to be left alone."[53] With the telephone number of the calling party, the called party can easily harass the calling party by calling back or even tracking down the name and address of the calling party.[54] While this may have some social benefit in allowing callers to quickly respond to obscene and annoying calls, I am nonetheless concerned that Caller ID *not* become a replacement for law enforcement intervention where criminal activity takes place. Further, Caller ID should not be allowed to lead to vigilantism in our communities if law enforcement involvement (through services such as "Call Trace") would be more appropriate.[55] One particularly compelling example of this danger is that of a battered wife calling home from a shelter to check upon the safety of her children. If the residence she calls has Caller ID, her own safety may be in danger.[56] Some representatives of law enforcement object to Caller ID because of the possibility of danger to their employees.[57] They argue that undercover agents would not be able to work from their homes for fear of the potential danger to their personal safety through Caller ID.[58]

---

ment that addressees file specific requests with post office before receiving mail from foreign countries which is considered "communist political propaganda"); Talley v. California, 362 U.S. 60 (1964)(struck ban on anonymous pamphleteering); NAACP v. Alabama, 357 U.S. 449 (1958)(state could not obtain NAACP membership list). *See also* Smith, *Caller Identification*, *supra* note 2, at 180-81.

53 Smith, *Caller Identification*, *supra* note 2, at 185.

54 *See, e.g.*, Sims, *Harassing Calls*, *supra* note 3, at 35.

55 *See supra* note 37.

56 *Telemarketing/Privacy Issues: Hearing Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce*, 102d Cong., 1st Sess. 49 (1991)(prepared statement of Janlori Goldman, Legislative Counsel, ACLU).

57 Curt Anderson, *Police, Bell Remain At Odds Over Caller ID Service*, Associated Press Wire Service, July 18, 1990.

58 The privacy concerns of the calling party will only increase in the future as new technologies such as personal communications networks (PCNs) become common. While "telecommuting," or working at home with telephones, faxes, and computers, is not yet widespread, it may become a substantial phenomenon in the coming decades. PCN, a technology in the trial stage, is a micro-cellular system in which persons would be given tiny portable telephones that they would carry with them. Instead of having a home or work number which is tied to a location, individuals would have personal telephone numbers tied to the individual, rather than a location. For both telecommuters and PCN users, their home numbers and work

2. The Called Party

If Caller ID only implicated privacy rights of the calling party, then there would be little debate about whether to allow the service. However, most parties involved with this issue, including me, recognize the utility of this service. Caller ID clearly contributes to two generally accepted social goods: greater public accountability from the calling party and greater privacy for the called party. It is worth noting that the notion that the calling party should not have to divulge his or her telephone number when making calls over the public telephone network does not go unchallenged. Supporters of Caller ID claim that the service is analogous to a peephole in one's door, allowing the person in the home to "see" who is knocking on the door, or, in the case of Caller ID, ringing the home telephone number.[59] While the two are not exactly comparable, the contention that both the telephone line and the doorway are the public's entrances to one's private residence, and thus need some sort of protection, is valid.

Professor Arthur Miller offers a different analogy to support his challenge to the expectation of privacy about one's telephone number:

> I believe that anonymity — not privacy — is what is being sought by a telephone caller who objects to having the telephone number revealed by Caller ID. The question then is whether a person has a right to hide behind a veil of anonymity in making a telephone call over the public telephone network . . . Society, for example, requires that automobiles have license plates to travel on a public road. This modest deprivation of anonymity is designed to promote accountability. Those who insist on anonymity in placing telephone calls are, in essence, saying they do not want to be accountable on the communications network, which is quite analogous to driving

---

numbers will become the same. This means that if they call someone who uses Caller ID, they would release both their home and business number, not just one or the other. Thus, for those telecommuters and PCN users who prefer not to give out their home numbers to those with whom they do business or vice-versa, Caller ID may pose an even greater concern down the road than for calling parties currently.

59 *Caller-ID Technology: Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. 267 (1990) (prepared statement of Harvard Law School Professor Arthur Miller). *See also* James E. Katz, *Caller-ID, Privacy and Social Processes*, TELECOMMUNICATIONS POLICY, October 1990, at 398.

without a license plate.[60]

Dr. Mark N. Cooper, the Director of Research for the Consumer Federation of America refutes the assertion that Caller ID is like driving a car with a license plates. Phone numbers provide much more information about a person. For instance,

> [i]n the course of a telephone call you may ask a question about a used car, want a price quote from a department store or seek advice from a rape crisis center. Revealing your telephone number in conjunction with these activities may link the number to very sensitive personal information.
>
> * * *
>
> My constituents, and survey after survey, tell me that the American people do not view their telephone numbers as license plates. They do not want to give up control over their numbers to the telephone company or anyone else. Many telephone companies insist that people give up control over their numbers because the companies will make much more money that way. Not only will a few consumers buy Caller ID, but all consumers will be forced to buy back their privacy by using credit cards, operators, phone booths, or other measures that the telephone companies will gladly sell.[61]

The anonymity that the telephone network presently allows comes at a certain cost to society. Obscene and harassing telephone callers are obviously one such cost. In New Jersey, for example, this cost may be gauged by the 72,000 requests that New Jersey Bell received from customers for help in dealing with annoyance calls in 1988.[62]

Caller ID helps reduce that cost to society by buttressing the "zones of privacy" of all individuals, even those who do not subscribe to the service. Caller ID gives the called party, who subscribes to caller ID, the ability to screen all calls, including those from problem callers, that intrude into one's residence. Additionally, the impact of Caller ID's availability is dramatic. New Jersey Bell has claimed that following installation of Caller ID in Hudson County, the number of reports of annoyance calls fell drastically, by

---

60 *Caller ID Technology: Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. 265-66 (1990).

61 *Telemarketing/Privacy Issues: Hearing Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce*, 102d Cong., 1st Sess. 41 (1991).

62 Sims, *Harassing Calls*, *supra* note 3, at A1 & 35

as much as forty-nine percent.[63] The mere knowledge of the availability of Caller ID service within a community among those individuals inclined to make such calls seems to be a potent deterrent that benefits all.

While Caller ID is an efficient way to screen calls, it may not be the most constructive response to obscene or harassing telephone calls. Although some have promoted it as a way to fight those types of calls, as I suggested earlier, such an approach may lead to vigilantism: the called party may use the telephone number to look up the offender's home address through reverse-directory assistance and then confront the calling party at the caller's home.[64] As noted, Call Trace, not Caller ID, might better be used to deal with those types of calls.[65] Call Trace sends the offender's number to the appropriate law enforcement authorities, who are clearly better equipped to deal with such a caller.[66]

3. Call Blocking

Another consideration is the availability of a CLASS feature known as "blocking" that addresses concerns regarding the impact of Caller ID on the privacy of the calling party. Blocking — either "per call" or "per line" — allows the calling party to prevent the display of his or her telephone number on the called party's Caller ID device. The difference is that per call blocking must be activated each time a person makes a call that he or she wants to be blocked, and per line blocking automatically blocks Caller ID displays for all calls made from that telephone line.[67]

---

[63] *Id.* at A1.

[64] Dr. Mark Cooper of the Consumer Federation of America testified that:

> What are people supposed to do with the telephone numbers of alleged harassers? In every PUC hearing I have been in, the telephone company suggests that they should call the alleged annoying caller back. That can be dangerous business. Just last week, I was on a radio talk show in which a man called and said he got even with an alleged harasser by calling back every hour for a day. He broke the law and what if he incorrectly copied the number from his Caller ID register? If the confrontation escalates into violence, does the telephone company bear some responsibility?

Hearing before the Subcommittee on Technology and the Law of the Senate Comm. on the Judiciary, 101st Cong., 2d Sess. 111 (1990).

[65] *See supra* note 37.

[66] *Id.*

[67] Per call blocking is activated by punching in a three digit code, such as "*67," as part of dialing a telephone number. With per line blocking, telephone company

Furthermore, I believe these blocking features do not undermine the value of Caller ID for the called party. If the calling party uses blocking, the called party will be alerted to this by a "B," for blocked, or some other means of denoting a blocked call, appearing on the Caller ID screen where a telephone number would normally appear, thus notifying the call recipient that the caller has blocked his or her number. With this information, the called party may elect not to answer a telephone call from a "blocking caller," thereby screening out all calls from individuals who will not identify themselves. Finally, those who use blocking to harass others may still be apprehended by using "Call Trace," which will provide the caller's telephone number to the phone company *regardless* of any attempt to block its transmission to the called party.

F. *Striking a Balance*

In order to properly balance the privacy interests of the calling and the called parties, the compromise legislation I have sponsored would require that, at a minimum, free per call blocking be offered in conjunction with Caller ID.[68] This balance protects the right to privacy of the calling party and also protects the privacy right of the called party. For the calling party, per call blocking preserves the right to informational privacy by giving the calling party control over the dissemination of his or her telephone number. It also protects the calling party's right to privacy because it allows anonymous telephone calls to be placed in certain circumstances in which there is a compelling social policy for such anonymity. For the called party, Caller ID is available to screen calls and thus enhance the privacy expectation of being "let alone" in one's home.

III. The Fair Credit Reporting Act

A more well-known clash between the privacy interests of consumers and the financial interests of business is the contro-

---

equipment automates that process for each call through a block put on the line at the telephone company's central office. *See* James E. Katz, *Caller-ID, Privacy and Social Process*, TELECOMMUNICATIONS POLICY, Oct. 1990, at 373.

68 Telephone Consumer Privacy Rights Act, H.R. 1305, 102d Cong., 1st Sess. § 3(b) (1991).

versy surrounding credit reports. The credit reporting industry dates from about the turn of the century, when local reporting services were formed mainly to benefit specific trades or industries. Although almost 2,000 local credit bureaus existed by the time of World War II, it was not until the post-war boom in consumer credit that their activities were scrutinized.[69]

As the popularity of credit cards increased in the late 1960's, Congress began to examine the types of information contained in credit bureau files and how that information was used. The result was the passage of the Fair Credit Reporting Act (FCRA)[70] on October 26, 1970.

It is now time for a comprehensive reform of the Fair Credit Reporting Act. Technological advances have reshaped the industry and allowed personal financial records to be widely distributed. New uses for data that was once only used to determine credit worthiness are appearing daily, and the advent of personal computers has made it possible for businesses of all sizes to utilize credit files.

A. *Technology and the Credit Reporting Industry*

When the Fair Credit Reporting Act went into effect in 1971 the credit reporting industry was still fairly primitive. Although some credit bureaus began to automate their files as early as 1965, most of them still maintained individual records on file cards. Checking an individual's credit required a phone call that took an average of three minutes.[71]

The need to manually check each file limited the activities of credit bureaus, thus the benefits of automation were apparent.

---

69 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 1st Sess. 227 (1991) (Statement of Walter R. Kurth, President of Assoc. Credit Bureaus, Inc.).

70 P.L. 91-508, 84 Stat. 1128, 15 U.S.C. §§ 1681-1681s (1988 & Supp. I 1988). See Jeffrey I. Langer & Andrew T. Semmelman, *Creditor List Screening Practices: Certain Implications Under the Fair Credit Reporting Act and the Equal Credit Opportunity Act*, 43 BUS. LAW. 1123 (1988) for an analysis of the prescreening provision of the FCRA.

71 *Fair Credit Reporting Act: Hearing before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 215 (1991) (Statement of Dr. Mary J. Culnan, Associate Professor of Business Administration, Georgetown University).

However, the costs associated with computerization were too high for most credit bureaus, and concentration was inevitable and rapid.

The three largest credit agencies were born of mergers and acquisitions. For example:

> [i]n less than five years, TRW has bought 33 other credit agencies, including [1988's] $330 million purchase of Chilton, which added 140 million files to TRW's computers. Equifax has put nearly 104 smaller credit bureaus on its network. Trans Union has brought aboard 23 and opened offices in 25 new markets. Together, the number of credit bureaus controlled by the Big Three has doubled during the 1980s to more than 200, giving them more than 90% of the U.S. adult population.[72]

In addition, the industry includes a number of "superbureaus," which buy credit files from a national data base and re-sell them. These companies market to smaller businesses that have an occasional use for credit information. The use of a superbureau is usually less costly than a direct membership in a major bureau. Any company or individual with a personal computer and a modem, who can come up with a reasonable explanation, has the ability to access credit files. As a direct result, although precautions are taken, many complaints about misused credit data can be traced back to superbureaus.[73]

B. *The Problem of Accuracy*

The three major systems receive information from banks and retailers, among others monthly, and each maintains an estimated 150 million files.[74] Each month, approximately two billion trade lines of credit history information and two million public record items are entered into the systems.[75]

---

72 Rothfeder, *Is Nothing Private?*, *supra* note 6, at 80.

73 Easy Access to Credit Reports Leads to a Scam, PRIVACY J. 1 (Mar. 1990). In addition, the *Business Week* reporter who gained access to Vice President Dan Quayle's credit history in 1989 used a superbureau. The reporter claimed to represent a non-existent company, and was approved to access the superbureau's data banks. Rothfeder, *Is Nothing Private?*, *supra* note 6, at 74-82.

74 Rothfeder, *Is Nothing Private?*, *supra* note 6, at 80.

75 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 2d Sess. 223 (1989) (statement of Walter R. Kurth).

With this huge volume of data, some mistakes are inevitable. The industry claims that only about 0.5% of the estimated 450 million credit reports used annually are changed because they are inaccurate.[76] However, several studies say that the actual error rate is far higher, and the volume of complaints that I have received in my office supports that contention.

In one 1988 study, Consolidated Information Services analyzed 1,500 credit reports from the three major data bases and found errors in 43% of the reports.[77] More recently, Consumers Union asked their staffers across the country to request their own credit files from all three of the major providers. Of the 161 reports that were reviewed, 48% had inaccuracies, and 19% had a major error.[78]

Although both of these studies used relatively small samples, the results suggest that many credit records are inaccurate. Since I became involved with this issue a couple years ago, I have been contacted by many people across the country who have been denied mortgages, credit, jobs and rental apartments because of mistakes on their credit records. In case after case, the credit bureaus were unresponsive and uninterested in helping them.

In one letter that I received, a New Jersey man was turned down for a mortgage because his credit report had sixteen separate errors. This included thirteen listed accounts that were not his. The credit bureau informed him that it would take six to eight weeks to correct the errors.

Even more shocking is the cavalier attitude that credit bureaus have shown towards these errors. In June 1991, a U.S. Public Interest Research Group study of complaints registered with the FTC found that over 60% of the consumers who wrote with unresolved complaints had already contacted the credit bureau five times or more. The average duration of their complaints was over twenty weeks.[79]

---

[76] *Id.* at 224.

[77] James Williams, CREDIT FILE ERRORS, A REPORT, CONSOLIDATED INFORMATION SERVICES, NEW YORK (Aug. 1989).

[78] WHAT ARE THEY SAYING ABOUT ME? THE RESULTS OF A REVIEW OF 161 CREDIT REPORTS FROM THE THREE MAJOR CREDIT BUREAUS, CONSUMERS UNION (April 29, 1991).

[79] NIGHTMARE ON CREDIT STREET II, A PROFILE OF CREDIT BUREAU COMPLAINT NIGHTMARES, UNITED STATES PUBLIC INTEREST RESEARCH GROUP (Washington, D.C., 1991).

Their findings are also in line with the complaints that my office has received or studied. Corrections can take months. Credit bureaus collect information by computer, but corrections are done by hand.

In the past, credit bureaus have kept costs down by making it hard for consumers to get and correct their files. In case after case, the consumer has to repeatedly call credit bureaus to get some action. Credit bureau personnel are often described as indifferent, incompetent or just plain nasty. Meanwhile, the innocent victims of credit bureau errors suffer.[80]

But to be fair, the errors are not always the credit bureaus' fault. Retail stores and card issuers are notoriously slow to list corrections or canceled accounts. The Fair Credit Reporting Act should explicitly require information providers to meet a strict standard of accuracy and timeliness.

Also, there is the issue of disclosure. Banks and even credit bureaus urge consumers to check their credit records regularly, or at least before making a major purchase. Then, however, the credit bureaus charge a hefty fee (usually $15 or more) before the consumer can get a copy of his or her credit history. Consumers should be able to get a free copy of their report at least annually.

Finally, creditors should be required to notify consumers whenever adverse information is sent to a credit bureau. This disclosure could be as simple as an additional line on the next statement, but it would prevent cases where a consumer is unaware of damaging information in his or her credit record.[81]

---

[80] On December 10, 1991, the FTC and TRW announced that they had agreed to the entry of a consent order over certain practices that violated the FCRA. Federal Trade Comm'n v. TRW, Inc., Civ. A. No. 3-91CV2661-H, 1991 WL 319694 (N.D. Tex. 1991). The original FTC suit charged that TRW did not exercise sufficient care to ensure that its credit reports were accurate; did not properly reinvestigate disputed information; allowed previously corrected errors to reappear in their files; furnished credit reports to individuals and organizations that did not have a permissible purpose to use them; and exercised insufficient care to ensure that reports that are used in hiring were accurate.

[81] These reforms are included in "The Credit Reporting Reform Act of 1991," H.R. 670, 102d Cong., 1st Sess. (1991), which I introduced in the House of Representatives on January 28, 1991 (the full text of H.R. 670 is set out in the appendix to this article).

C. *Pre-Screening*

Although credit files are mainly collected in order to help lenders make informed decisions on future credit requests, the information is also sold to third parties. Credit files are used to compile mailing lists that can be used to market both additional credit products and a wide variety of other products. In general, all of these uses can be grouped under the term "pre-screening."[82]

Pre-screening began long before credit bureaus began to use computers. Credit bureaus would take mailing lists supplied by third parties, and manually eliminate names that did not meet a pre-determined set of qualifications. However, this was a lengthy process and it was not practical in most situations.

Most discussions of pre-screening concentrate on the use of credit data to market other credit products; this is often not the case. Today, pre-screened data is used to develop marketing plans or to better target mass mailings. The most common use is in direct marketing, where purchased mailing lists can be screened for extremely explicit criteria. It would be possible to develop a mailing list that was limited to homeowners in Union, New Jersey, who have incomes of over $50,000, prefer to use department store charge accounts instead of bank cards, and have over $10,000 of unused credit available.[83] Marketers claim that pre-screening allows them to limit their mailings to customers that are most likely to be interested in their products and that are most likely to be able to pay for them.[84]

Other uses of credit data include developing lists of credit customers who have a high probability of bankruptcy or delinquency.[85] When credit data is matched with other information in a bureau's files, a marketer can discover geographic areas with the best credit prospects, the amount of credit available in an

---

82 *See Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 222 (1991)(prepared testimony of Dr. Mary J. Culnan).

83 *See generally* Rothfeder, *Is Nothing Private?*, *supra* note 6, at 76.

84 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 460-62 (1991)(letter from Richard A. Barton, Senior Vice President, Government Affairs, Direct Marketing Association, Inc. to The Honorable Esteban E. Torres, June 6, 1991).

85 Rothfeder, *Is Nothing Private?*, *supra* note 6, at 74.

area, and the market share of each creditor by zip code.[86]

The advent of computers made pre-screening both easier and more necessary. The increasing cost of purchasing and maintaining high speed computers has proved to be a strong incentive for credit bureaus to find new ways to sell credit data to third parties.

Typically, a marketer will contract with a credit bureau to either screen an existing mailing list or to develop a new one. Solicitations to names on the pre-screened list may be sent by the marketer, the credit bureau, or an independent mailing service.[87]

Many credit bureaus respond to privacy concerns about pre-screening by claiming that their credit data bases are kept separate from their marketing data.[88] However, the reality is often different. One seller of marketing data admits to using its credit files to update and enhance its demographic files. In addition to updating addresses and phone numbers, concise summaries of credit information are also regularly added to the files.[89] Marketers have found that combining several data bases together provides a complete picture of a prospective customer's financial condition and lifestyle.

Credit bureaus often claim that a consumer's privacy is further protected because they only send pre-screened lists to a mailing service and not to the marketer. However, these mailing services may further refine the pre-screened lists by using demographic or other data before using them,[90] and it is possible for

---

86 These and other services are described in "Leading the Way," a Trans-Union Credit Information Co. promotional brochure. *Amendments to the Fair Credit Reporting Act: Hearing before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 2d Sess. 809-28 (1990). *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 1st Sess. 273 (1989) (statement of Walter R. Kurth).

87 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 404-06 (1991) (prepared statement of VISA U.S.A., Inc., and Mastercard International, Inc.).

88 TRW, for instance, keeps its credit data files in California and its marketing data base in Texas.

89 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 222-23 (1991)(prepared statement of Dr. Mary J. Culnan).

90 *Id.* at 407 (prepared statement of VISA U.S.A., Inc. and Mastercard International, Inc.).

them to retain a copy.

D. *The Legal Basis for Pre-Screening*

The FCRA allows the release of a credit report in several narrow circumstances.[91] Prescreening is allowed under a controversial 1972 interpretation of Section 604 of the FCRA by the Federal Trade Commission.[92]

Even those who support pre-screening concede that there is

---

[91] 15 U.S.C. § 1681b provides

> A consumer reporting agency may furnish a consumer report under the following circumstances and no other:
>
> (1) In response to the order of a court having jurisdiction to issue such an order.
>
> (2) In accordance with written instructions of the consumer to whom it relates.
>
> (3) To a person which it has reason to believe—
>
> (A) intends to use the information in connection with credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or
>
> (B) intends to use the information for employment purposes; or
>
> (C) intends to use the information in connection with the underwriting of insurance involving the consumer; or
>
> (D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or
>
> (E) otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.

[92] 38 Fed. Reg. 4945-47 (1973). *See* Sheldon Feldman, *The Current Status of the Law Governing Prescreening, Including Permissible Postscreening Practices*, 46 Bus. Law. 1113, 1114 (1991) [herinafter Feldman, *Current Status of Prescreening*]. Feldman states that the FTC prescreening interpretation of FCRA received a lot of attention. He describes the "basic rationale for the [i]terpretation":

> [P]rescreening involves accessing credit bureau files, a practice which is not permitted under section 604 of the FCRA unless the person seeking access has one of the specified 'permissible purposes' to receive such information . . . The FCRA applies to this practice because, technically, the prescreened list of consumers' names and addresses constitutes a series of 'consumer reports' (i.e., information collected by a consumer reporting agency about a consumer that bears on his creditworthiness). To give effect to such . . . a list would be justifiable if the creditor would certify that every person who passed the prescreen would receive an offer of credit. The offer of credit was deemed to establish the 'permissi-

little, if any, legislative history on either side of the issue.[93] After a long debate, the FTC decided to allow pre-screening, but placed a restriction on it: "The user of a consumer report must be considering a business transaction involving each consumer upon whom a credit report is furnished."[94] In other words, credit files could not be accessed for informational purposes, but only in conjunction with a specific offer of credit or services.[95]

The FTC concedes that the statute could be interpreted as allowing the use of credit reports only in transactions that are initiated by the consumer.[96] However, the FTC also notes that the statute does not limit itself to consumer-initiated transactions.[97]

Under both the 1972 FTC interpretation of the Fair Credit Reporting Act, and the recent 1990 re-interpretation[98], a firm of-

---

ble purpose' without which it would be lawful to obtain a consumer report.

Id. at 1114.

See also Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs, 102d Cong., 1st Sess. 220-21 (1991)(prepared statement of Dr. Mary J. Culnan).

93 *Fair Credit Reporting Act: Hearing before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 1st Sess. 238 (1989)(statement of Walter R. Kurth).

94 16 C.F.R. § 600.5(d)(1989). In 1990 the FTC reinterpreted the FCRA and whether prescreening was permissible. The FTC stated:

> [p]resceening is permissible under the FCRA if the client agrees in advance that each consumer . . . receive an offer of credit. In theses circumstances, a permissible purpose for the prescreening service exists under this section, because of the client's present intent to grant credit to all consumers of the final list, with the result that the information is used 'in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to . . . the consumer.'

55 Fed. Reg. 18815 (1990)(codified at 16 C.F.R. § 600 app. (1991)). See Feldman, *The Current Status of Prescreening supra* note 92, at 1117-19 for a discussion on the current FTC position on prescreening.

95 Feldman, *Current Status of Prescreening, supra* note 92, at 1117.

96 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 1st Sess. 944 (1989) (written responses by Janet D. Steiger, Chairperson of Federal Trade Commission to additional questions submitted by the Subcommittee).

97 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 2d Sess. 184 (1991)(prepared statement of Jean Noonan, Associate Director for Credit Practices, Bureau of Consumer Protection, FTC).

98 *See supra* note 92.

fer of credit must be made to every person whose name appears on a pre-screened mailing list.[99] The FTC had considered requiring the actual extension of credit to be made, but was dissuaded because an individual's circumstances could change between the creation of a mailing list and the consumer's reply to an offer of credit.[100]

I believe that the FTC incorrectly interpreted the law, and that pre-screening is not allowable under the law. My belief is based on an analysis of the statute by the Congressional Research Service.[101] I also believe that using credit records to develop marketing plans or mailing lists is illegal.

Credit bureaus and marketers claim that consumers are not damaged by pre-screening, since if they do not meet the criteria for a certain list, their credit file is not adversely affected. They also state that since only names and addresses are provided, and that checking is done by computers, a consumer's privacy has not been compromised.[102] I believe that this contention is both mistaken and misses the point of the entire debate over privacy.

The Fair Credit Reporting Act applies to any pre-screened list that is derived from information in a consumer's credit history files. The FTC holds that the application of the Act depends on the source of the information and not its contents.[103]

Under this interpretation, I believe that the credit bureau's practice of transferring information from its credit files to its marketing files makes both files credit reports. The industry may contend that they are just updating names and addresses, but

---

99 The 1990 FTC interpretation is somewhat more liberal, in that a credit provider is allowed to vary the terms of the credit offer depending on the determination of the consumer's credit worthiness. 16 C.F.R. § 600 app. (1991).

100 *Fair Credit Reporting Act: Hearing Before the Subcomm. of Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 1st Sess. 239 (1989)(prepared statement of Walter Kurth).

101 *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 102d Cong., 1st Sess. 688 (1991)(report of Congressional Research Service, Fair Credit Reporting Act: Comparison of 102d Congress Bills and Current Law (1991)).

102 *Id.* at 461 (letter from Richard A. Barton, Senior Vice President, Government Affairs, Direct Marketing Association, Inc. to The Honorable Esteban E. Torres).

103 *The Fair Credit Reporting Act: Hearing before the Subcomm. on Consumer Affairs and Coinage of the House Comm. on Banking, Finance and Urban Affairs*, 101st Cong., 1st Sess. 974 (1989) (written responses by the FTC to additional questions by Representative Charles E. Schumer).

since credit files are the source, any use of those files must comply with the Fair Credit Reporting Act.

However, I would prefer to go even further. As I stated earlier in this article, the Fourth Amendment gives consumers rights over the subsequent disclosure of personal information.[104] It is unlikely that the FTC will change its opinion on the legality of pre-screening unless the statute is clarified. As a result, I believe that the Fair Credit Reporting Act should be amended to allow credit files to be used only in transactions initiated by the consumer.[105]

IV. Conclusion: Computers and Privacy in the Future

Privacy concerns raised by both Caller ID and the use of credit records are the direct result of sophisticated telecommunications and computer technology. Both situations developed slowly over time, and in neither case was there any criminal intention to violate the privacy right of individuals.

It would be unrealistic and even foolish to expect the growth in telecommunications and computer sophistication to end, or to propose restricting it. It would be equally naive, however, to assume that there will be no need to provide additional privacy protections nor to continually re-examine the laws governing the use of personal information.

As more records become automated, people will find a use for them. Twenty years ago no one would have expected the change-of-address card files with a post office or applications for a drivers license to be routinely provided to credit bureaus. However, this is now fact.

Just as we expect each new generation of computer technology to have a limited lifetime, we must recognize that the legal structure of the past may no longer provide the necessary amount of protection. To some extent, this can be remedied by allowing regulatory agencies to interpret the law through regulations, but as our experience with pre-screening shows, areas where the law is silent or ambiguous can develop into massive loopholes.

Thomas Jefferson is reported to have said "eternal vigilance

---

104 *See supra* note 47.

105 *See* H.R. 670, 102d Cong., 1st Sess. § 3 (1991).

is the price of liberty."[106] He did not have computers in mind, but the sentiment certainly applies.

---

[106] RESPECTFULLY QUOTED, A DICTIONARTY OF QUOTATIONS REQUESTED FROM THE CONGRESSIONAL RESEARCH SERVICE 205 (Suzy Platt ed. 1989).

I

102D CONGRESS
1ST SESSION

H. R. 670

To amend the Fair Credit Reporting Act to provide greater disclosure to consumers of information concerning consumers by creditors, credit reporting agencies, and other users of credit information, prevent abuses with regard to such information, to increase the enforcement authority of Federal regulatory agencies with responsibility to enforce the Fair Credit Reporting Act, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 28, 1991

Mr. RINALDO (for himself and Mr. SHAYS) introduced the following bill; which was referred to the Committee on Banking Finance and Urban Affairs

---

A BILL

To amend the Fair Credit Reporting Act to provide greater disclosure to consumers of information concerning consumers by creditors, credit reporting agencies, and other users of credit information, prevent abuses with regard to such information, to increase the enforcement authority of Federal regulatory agencies with responsibility to enforce the Fair Credit Reporting Act, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Credit Reporting Reform Act of 1991".

SEC. 2. DISCLOSURE REQUIREMENTS.

(a) DISCLOSURES REQUIRED OF CREDITORS AND OTHER USERS OF CONSUMER CREDIT INFORMATION.—Section 609(b) of the Fair Credit Reporting Act (15 U.S.C. 1681g(b)) is amended to read as follows:

"(b) DISCLOSURES BY CREDITORS.—

"(1) DISCLOSURE AT BEGINNING OF CREDIT TRANSACTION.—Before extending any credit under any open end consumer credit plan, issuing any charge card, or engaging in any consumer credit transaction other than under an open end consumer credit plan, any creditor or charge card issuer shall provide the consumer with a written notice containing a description of—

"(A) the circumstances under which the creditor or charge card issuer will provide any consumer reporting agency with any information concerning the consumer; and

"(B) the type of information which will be provided to any such agency under such circumstances.

"(2) NOTICE THAT INFORMATION HAS BEEN REPORTED.—If any creditor or charge card issuer furnishes any information with respect to any consumer to any consumer reporting agency, the creditor or charge card issuer shall provide notice of such fact—

"(A) in the next statement mailed to the consumer; or

"(B) in writing to the consumer before the end of the forty-five-day period beginning on the date the information is furnished to the agency.

"(3) DEFINITIONS.—For purposes of this subsection, the terms 'creditor' and 'open end credit plan' have the meanings given to such terms in section 103 of the Truth in Lending Act.".

(b) CONSUMERS ENTITLED TO COPIES OF INFORMATION IN CONSUMERS' FILES ON DEMAND.—Section 609(a)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681g(a)(1)) is amended to read as follows:

"(1) All information in the agency's files on the consumer at the time of the request.".

(c) INFORMATION REQUIRED TO BE PROVIDED WITHOUT CHARGE.—Section 612 of the Fair Credit Reporting Act (15 U.S.C. 1681j) is amended to read as follows:

"SEC. 612 NO CHARGES ALLOWED FOR DISCLOSURES TO CONSUMERS.

"No consumer reporting agency may impose any charge or fee on any consumer for any disclosure to—

"(1) such consumer under section 609 or 611(d); or

"(2) any person designated by the consumer under section 611(d).".

(d) DISCLOSURES REQUIRED FOR ANY ADVERSE ACTION BASED ON A CONSUMER CREDIT REPORT.—Subsection (a) of section 615 of the Fair Credit Reporting Act (15 U.S.C. 1681m) is amended to read as follows:

"(a) NOTICE OF ADVERSE ACTIONS BASED ON CREDIT REPORTS.—

"(1) IN GENERAL.—Any person which—

"(A) obtains a consumer report on any consumer from any consumer reporting agency; and

"(B) takes any action which is—

"(i) adverse to any interest of the consumer; and

"(ii) based on whole or in part on any information contained in such report.

shall provide written notice of the adverse action to the consumer.

"(2) CONTENTS OF NOTICE.—The notice provided by any person to any consumer pursuant to paragraph (1) shall contain—

"(A) a copy of the consumer report on the consumer;

"(B) the name and address of the consumer reporting agency which furnished the report to such person;

"(C) the name and address of each of the three largest consumer reporting agencies; and

"(D) a description of the consumer's rights under this title.".

SEC. 3. LIMITATIONS ON PERMISSIBLE USES OF CONSUMER REPORTS.

"(a) LEGITIMATE BUSINESS USE AVAILABLE ONLY FOR CONSUMER INITIATED TRANSACTIONS.—Section 604 of the Fair Credit Reporting Act (15 U.S.C. 1681b) is amended—

"(1) in paragraph (3)(E), by striking 'involving' and inserting 'initiated by';

"(2) by striking 'A consumer reporting agency' and inserting

"(a) IN GENERAL.—Subject to subsection (b), a consumer reporting agency"; and

"(3) by adding at the end the following new subsection:

"(b) NO INFORMATION MAY BE PROVIDED OTHER THAN A CONSUMER REPORT.—No consumer reporting agency may provide or use any information concerning any consumer, including the name and address of any consumer,

for any purpose, including the creation of marketing plans or mailing lists, other than in connection with providing a consumer report on such consumer to the extent permitted under subsection (a).".

(b) OPEN ENDED CONSUMER RELEASES PROHIBITED.—Section 615 of the Fair Credit Reporting Act (15 U.S.C. 1681m) is amended by adding at the end the following new subsection:

"(d) OPEN ENDED CONSUMER RELEASES PROHIBITED.—No user of any consumer report on any consumer may require or permit the consumer to authorize the user to obtain any consumer report or other information on the consumer from any consumer reporting agency after the end of the completion of the transaction or the termination of the credit relationship between the user and the consumer for which the user initially obtains a consumer report on such consumer.".

SEC. 4. LIMITATION ON INFORMATION WHICH MAY BE CONTAINED IN ANY CONSUMER REPORT.

(a) IN GENERAL.—Section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)) is amended by striking "of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and inserting "by any consumer re-

porting agency of factual information on any consumer's payment records and accurate legal and financial information directly relating to such consumer".

(b) GRADUATED PERIODS OF OBSOLESCENCE FOR CERTAIN INFORMATION.—Section 605(a)(6) of the Fair Credit Reporting Act (15 U.S.C. 1681(a)(6)) is amended to read as follows:

"(6) Information relating to late or overdue payments as follows:

"(A) Payments which were not more than thirty days overdue on the date of payment and were made more than three years before the date of the report.

"(B) Payments which were more than thirty days but not more than sixty days overdue on the date of payment and were made more than four years before the date of the report.

"(C) Payments which were more than sixty days but not more than ninety days overdue on the date of payment and were made more than five years before the date of the report.

"(D) Payments which were more than ninety days overdue on the date of payment and were made more than seven years before the date of the report.".

(c) AMENDMENT TO EXEMPTION FROM OBSOLETE INFORMATION LIMITATION.—Section 605(b) of the Fair Credit

Reporting Act (15 U.S.C. 1681c(b)) is amended to read as follows:

"(b) EXEMPTION FOR CERTAIN LIFE INSURANCE POLICIES.—Subsection (a) shall not apply with respect to any consumer report which is furnished to any person in connection with the underwriting by such person of any life insurance policy which has a face amount, or which may reasonably be expected to have a face amount, of $50,000 or more.".

(d) PROMPT REINVESTIGATION OF DISPUTED INFORMATION REQUIRED.—Section 611(a) of the Fair Credit Reporting Act (15 U.S.C. 1681i(a)) is amended by striking "within a reasonable period of time" and inserting ", before the end of the thirty-day period beginning on the date the consumer files notice of such dispute with the agency".

(e) CONSUMER REPORTING AGENCIES REQUIRED TO CORRECT PRIOR INACCURATE OR INCOMPLETE REPORTS.—Section 611(a) of the Fair Credit Reporting Act (15 U.S.C. 1681i(a)) is amended—

(1) in the 1st sentence—

(A) by striking ", at the request of the consumer,"; and

(B) by striking "to any person designated by the consumer" and all that follows through the period and inserting "to any person to whom such

information was provided by the agency within the preceding one-year period."; and

(2) by striking the second sentence.

(f) STUDY REQUIRED ON IMPROVING ACCURACY OF INFORMATION IN CONSUMER FILES.—

(1) STUDY.—The Federal Trade Commission shall conduct a study on procedures for consumer reporting agencies to follow which allow such agencies to achieve maximum possible accuracy in the information collected and maintained in consumer files.

(2) REPORT TO CONGRESS.—Before the end of the twenty-four-month period beginning on the date of the enactment of this Act, the Federal Trade Commission shall submit a report to the Congress containing the findings and conclusions of the commission with respect to the study required under paragraph (1), together with such recommendations for administrative or legislative action as the commission may determine to be appropriate to implement the recommended procedures.

SEC. 5. CIVIL MONEY PENALTIES AND ADMINISTRATIVE ENFORCEMENT.

(a) CIVIL MONEY PENALTIES ESTABLISHED.—Section 621 of the Fair Credit Reporting Act (15 U.S.C. 1681s) is amended by adding at the end the following new subsection:

"(d) CIVIL MONEY PENALTIES.—

"(1) PENALTY IMPOSED.—Any person who violates any provision of this title shall forfeit and pay a civil penalty of not more than $10,000 for each day during which such violation continues.

"(2) ASSESSMENT.—Any penalty imposed under paragraph (1) may be assessed by the appropriate agency referred to in subsection (a) by written notice at any time before the end of the seven-year period beginning on the date the violation occurred (or, in the case of a continuing violation, the last date on which the violation occurred).

"(3) CIVIL ACTION.—Any agency which assesses a civil penalty under this subsection may commence a civil action to recover such penalty at any time before the end of the two-year period beginning on the later of—

"(A) the date on which the penalty was assessed; or

"(B) the date any judgment becomes final under section 619 or 620 in connection with the same violation with respect to which the penalty is assessed.

"(4) AUTHORITY TO MODIFY OR REMIT PENALTY.—The appropriate agency referred to in subsection

(a) may compromise, modify, or remit any penalty which such agency may assess or had already assessed under paragraph (1).

"(5) DISBURSEMENT.—All penalties collected under this subsection shall be deposited into the Treasury.".

(b) REGULATORY AUTHORITY OF FTC.—The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended by redesignating section 622 as section 624 and by inserting after section 621 the following new section:

"SEC. 622. REGULATIONS.

"The Federal Trade Commission shall prescribe such regulations, after notice and opportunity for comment, as may be necessary to carry out the requirements of this title and prevent evasions of any provision of this title.".

(c) REGISTRATION WITH FTC.—The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended by inserting after section 622 (added by subsection (b) of this section) the following new section:

"SEC. 623. REGISTRATION WITH FTC OR OTHER APPROPRIATE AGENCY.

"(a) IN GENERAL.—Each consumer reporting agency and each person who furnishes any information on any consumer to any such agency shall register with the Federal Trade Commission or the appropriate agency referred to in

section 621(a) as a consumer reporting agency or furnisher of information to any consumer reporting agency.

"(b) UNREGISTERED PERSONS PROHIBITED FROM ENGAGING IN CREDIT REPORTING.—Only any person who—

"(1) is registered as a consumer reporting agency in accordance with subsection (a) may provide any consumer report on any consumer to any person; and

"(2) is registered as a furnisher of information may provide any information concerning any consumer to any consumer reporting agency.".

(d) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) Section 616 of the Fair Credit Reporting Act (12 U.S.C. 1681n) is amended by inserting ", person who furnishes information to any consumer reporting agency," after "consumer reporting agency".

(2) Section 617 of the Fair Credit Reporting Act (12 U.S.C. 1681o) is amended by inserting ", person who furnishes information to any consumer reporting agency," after "consumer reporting agency".

(e) CLERICAL AMENDMENT.—The table of sections for title VI of the Consumer Credit Protection Act is amended by redesignating the item relating to section 622 as section 624 and inserting after the item relating to section 621 the following new items:

"622. Regulations.
"623. Registration with FTC or other appropriate agency.".

IB

Union Calendar No. 191

102D CONGRESS
1ST SESSION

H. R. 1305

[Report No. 102–324]

To amend the Communications Act of 1934 to protect the privacy rights of telephone subscribers.

IN THE HOUSE OF REPRESENTATIVES

MARCH 6, 1991

Mr. MARKEY (for himself, Mr. RICHARDSON, Mr. SLATTERY, Mr. COOPER, and Mr. FRANK of Massachusetts) introduced the following bill; which was referred to the Committee on Energy and Commerce

NOVEMBER 18, 1991

Additional sponsors: Mr. GORDON, Mr. LEHMAN of California, Mr. LAFALCE, Mrs. BOXER, Mr. TOWNS, Ms. KAPTUR, Mr. KOLBE, Mr. BRYANT, Mr. KOLTER, Mr. ECKART, Mr. ABERCROMBIE, Mrs. MEYERS of Kansas, Mr. SCHUMER, and Mr. OBERSTAR

NOVEMBER 18, 1991

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on March 6, 1991]

A BILL

To amend the Communications Act of 1934 to protect the privacy rights of telephone subscribers.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Telephone Consumer Privacy Rights Act".

SEC. 2. FINDINGS.

The Congress finds that:

(1) The right of privacy is the central principle that should guide the introduction and use of new telecommunications technologies and services.

(2) Caller Identification Service, known as "Caller ID", can provide value to telephone subscribers by identifying the calling party prior to accepting the call.

(3) Interexchange carriers offering "800" and "900" number services often pass a protocol service known as the Automatic Number Identification ("ANI") that identifies the calling party's telephone number to end users.

(4) While Caller ID provides value to the called party, it also affects the legitimate privacy interests of the calling party.

(5) These privacy interests must be properly balanced to protect the rights of both calling and receiv-

ing party when caller identification services are offered by common carrier.

(6) This personal information can be developed into highly sophisticated and possibly intrusive lists that are subsequently used or sold for marketing and other purposes often without the knowledge or consent of consumers whose information was accessed initially through Caller ID or ANI generated information.

(7) Unrestricted offerings of caller identification services may infringe upon some calling parties' expectations of anonymity and privacy in some or all of their telephone transactions.

(8) Federal requirements for the offering of caller identification service are necessary to ensure uniformed regulation which appropriately balance the rights of both the calling and receiving party when caller identification services are offered by common carriers.

SEC. 3. CUSTOMER PRIVACY REQUIREMENTS.

(a) AMENDMENT.—Title II of the Communications Act of 1934 is further amended by adding at the end thereof the following new section:

"SEC. 227. CUSTOMER PRIVACY REQUIREMENTS.

"(a) DEFINITIONS.—As used in this section—

"(1) The term 'caller identification service' means a service which makes use of a display device at the called party's telephone to automatically indicate the local telephone number (with or without the area code) of any party calling from within the local area or from another area, except that such term does not include an automatic number identification service.

"(2) The term 'automatic number identification' means an access signaling protocol in common use by common carriers that uses an identifying signal associated with the use of subscriber's telephone to provide billing information or other information to the local exchange carrier and to any other interconnecting carriers.

"(3) The term 'aggregate information' means collective data that relates to a group or category of services or customers, from which individual customer identities or characteristics have been removed.

"(b) CALLING PARTY IDENTIFICATION.—

"(1) RULEMAKING REQUIRED.—The Commission shall, within 180 days after the date of enactment of this section, prescribe regulations requiring any caller identification service offered by a common carrier, or by any other person that makes use of the facilities

of a common carrier, to allow the caller to withhold, on a per-call basis, the display of the caller's telephone number, name, or other personally identifying information, from the telephone or other instrument of the individual receiving the call.

"(2) CHARGES FOR WITHHOLDING NUMBERS PROHIBITED.—Such regulations shall prohibit any charges from being imposed on the caller who requests that his or her telephone number be withheld from the recipient of a call placed by the caller.

"(3) NOTIFICATION TO CUSTOMERS.—Such regulations shall require every common carrier to notify its subscribers that their calls may be identified to a called party not later than—

"(A) 30 days before the common carrier commences to participate in the offering of a call identification service; and

"(B) 60 days after the date such regulations are prescribed, if the private or common carrier is participating in the offering of a call identification service prior to such date.

"(4) EXEMPTIONS.—This subsection does not apply to any of the following:

"(A) A caller identification service which is used solely in connection with calls within the

same limited system, including (but not limited to) a Centrex, virtual private network, or private branch exchange system.

"(B) A caller identification service which is used on a public agency's emergency telephone line or on the line which receives the primary emergency telephone number (911) or on any entity's emergency assistance poison control telephone line.

"(C) A caller identification service provided in connection with legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency.

"(5) WAIVER.—The regulations prescribed by the Commission under paragraph (1) may waive the requirements of this subsection where compliance with such requirements is not technologically feasible.

"(c) AUTOMATIC NUMBER IDENTIFICATION SERVICES.—

"(1) CONTRACT REQUIREMENTS.—Any common carrier or affiliate of a common carrier providing automatic number identification services to any person shall provide such services under a contract or tariff containing telephone subscriber information re-

quirements that comply with this subsection. Such requirements shall—

"(A) permit such person to use the telephone number and billing information provided pursuant to the automatic number identification service for billing and collection, routing, screening, and completion of the originating telephone subscriber's call or transaction, or for services directly related to the originating telephone subscriber's call or transaction;

"(B) prohibit such person from reusing or selling the telephone number or billing information provided pursuant to the automatic number identification service without first orally (i) notifying the originating telephone subscriber and (ii) extending to such subscriber the option to limit or prohibit such reuse or sale;

"(C) prohibit such person from disclosing, except as permitted by subparagraphs (A) and (B), any information derived from the automatic number identification service for any purpose other than—

"(i) performing the services or transactions that are the subject of the originating telephone subscriber's call,

"(ii) ensuring network performance, security, and the effectiveness of call delivery,

"(iii) compiling, using, and disclosing aggregate information, and

"(iv) complying with applicable law or legal process.

"(2) EXCEPTION FOR ESTABLISHED CUSTOMERS.—The customer information requirements imposed under paragraph (1) shall not prevent a person to which automatic number identification services are provided from using—

"(A) the telephone number and billing information provided pursuant to such service, and

"(B) any information derived from the automatic number identification service, or from the analysis of the characteristics of a telecommunications transmission,

to offer, to any telephone subscriber with which such person has an established customer relationship, a product or service that is directly related to the products or service previously acquired by that customer from such person.

"(3) ENFORCEMENT.—(A) Each common carrier shall receive and transmit to the Commission complaints concerning violations of the telephone sub-

scriber information requirements imposed under paragraph (1). Each common carrier shall submit to the Commission, in such form as the Commission may require by regulation, reports on actions taken by the carrier to comply with this section.

"(B) The Commission may, by rule or order, direct the termination of automatic number identification services to any person who has violated the telephone subscriber information requirements imposed under paragraph (1). For purposes of section 503(b)(1)(B), violations of such requirements shall be considered to be a violation of a provision of this Act.

"(4) EFFECTIVE DATE.—(A) Except as provided in subparagraph (B), the requirements of this subsection shall apply to any automatic number identification service provided on or after one year after the date of enactment of this subsection.

"(B) In the case of any automatic number identification service provided under a contract entered into, or tariff taking effect, more than 90 days after the date of enactment of this subsection, the requirements of this subsection shall apply to any automatic number identification service provided pursuant to such contract or tariff.

"(d) STATE LAW.—Notwithstanding any other provision of this Act, no State shall prohibit or effectively prevent the provision of caller identification services.".

SEC. 4. CONFORMING AMENDMENT.

Section 2(b) of the Communications Act of 1934 is amended by striking "Except as provided" and all that follows through "and subject to the provisions" and inserting "Except as provided in sections 223 through 227, inclusive, and subject to the provisions".

SEC. 5. BLOCKING.

Nothing in this Act shall be construed to prevent a common carrier, or any other person that makes use of the facilities of a common carrier, from offering services or technology enabling a telephone subscriber receiving a call to block the call, or block the completion of the call where the caller has chosen to withhold the display of the caller's telephone number, name, or other personally identifying information.