UIC John Marshall Journal of Information Technology & Privacy Law

Volume 7
Issue 1 *Computer/Law Journal - Summer 1986*

Article 4

Summer 1986

The Threat from Within: Cable Television and the Invasion of Privacy, 7 Computer L.J. 89 (1986)

Glen R. Segal

THE THREAT FROM WITHIN: CABLE TELEVISION AND THE INVASION OF PRIVACY

By late 1983, cable television reached 40.5% of the eighty-three million American homes.[1] It is estimated that sixty to seventy percent of all homes will have cable television by 1990.[2] One type of cable system gaining popularity is the interactive or "two-way" cable system. In an interactive system, the subscriber's television is connected to a central computer at the cable company or "head end." The subscriber controls the system with a keypad console that is attached to the television set. By pressing the buttons on the console, the subscriber is able to "talk back" to the computer at the head end.[3]

One of the first interactive systems installed was Warner Amex's QUBE system in Columbus, Ohio, in the 1970's. Since then, QUBE has been installed in a number of cities, such as Cincinnati and Pittsburgh. Other cable companies are also installing their own interactive systems, such as Cox Cable Communications' INDAX system.

Interactive cable provides a number of different services. Besides showing movies, interactive cable offers or will offer its subscribers banking and shopping services, information retrieval, pay-per-view programs, home security and smoke detectors, and public opinion polling.[4] As a result of this technology, vast amounts of personal information will flow from the subscriber's television to the cable company. Congress has recognized that the "[s]ubscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions."[5] Because of the flow of such personal information, interactive cable technology presents a tremendous threat to personal privacy.

---

1. Kerr, *Consumer Complaints on Service Plague Cable Television Industry*, N.Y. Times, Dec. 26, 1983, § 1, at 1, col. 2.

2. *Id.*

3. *See* Wicklein, *Wired City, U.S.A.*, ATL. MONTHLY, Feb. 1979, at 35, 36.

4. *See* Davis, *Current Regulatory Changes and Business Developments in the United States' Communications Industry*, in CABLE TELEVISION IN A NEW ERA 44-45 (1983). *See also* Note, *As Interactive Cable Enters, Does Privacy Go Out the Window?*, 4 COMM/ENT 781, 791 (1982) [hereinafter Note, *Interactive Cable*].

5. H.R. REP. NO. 934, 98th Cong., 2d Sess. 29, *reprinted in* 1984 U.S. CODE CONG. & ADMIN. NEWS 4655, 4666.

This Note will explore the various ways in which interactive cable poses a threat to privacy. This Note will then explore the various remedies available to the subscriber if his privacy has in fact been invaded. Finally, this Note will propose a solution to combat the potential threat to individual privacy from cable television.

I. CABLE TELEVISION AS A THREAT TO PRIVACY

A majority of Americans are concerned that various new technologies threaten individual privacy. According to a recent Harris poll, sixty-nine percent of the people surveyed believed that we were "at least somewhat close" to a "big brother" state as depicted by George Orwell.[6] In fact, Orwell could have been describing interactive cable when he wrote the following in his futuristic novel, *1984*:

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[7]

A workable definition of privacy must be established before one can discuss how cable can invade one's privacy. One theory of privacy is that privacy is the "control we have over information about ourselves."[8] Thus, the more control we have over the release of personal information, the more privacy we enjoy. It has been argued that when an individual is deprived of the control of personal information, "he becomes subservient to those people and institutions that are able to manipulate [such information]."[9] Because individuals fear that their private lives may be turned into public spectacles,[10] the possessors of such information could control those individuals through either blackmail or blacklisting.

---

6. *Privacy and 1984: Hearing Before the Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations*, 98th Cong., 1st Sess. 7 (1984) (statement of Louis Harris) [hereinafter *Privacy Hearing*].

7. G. ORWELL, 1984 6-7 (Signet Classic ed. 1961).

8. Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (emphasis omitted).

9. A. MILLER, THE ASSAULT ON PRIVACY 25 (1971). *See also* K. GREENAWALT, LEGAL PROTECTIONS OF PRIVACY x (1975).

10. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1006 (1964).

If individuals do not have control over personal information, their behavior could change because

> [i]f we thought that our every word and deed were public, fear of disapproval or more tangible retaliation might keep us from doing or saying things which we would do or say if we could be sure of keeping them to ourselves or within a circle of those who we know approve or tolerate our tastes.[11]

This change in behavior would tend to produce conformity and to reduce dissent because of the fear of being shunned or retaliated against.[12] Such a fear would not exist if individuals were able to maintain control over personal information. In order to preserve individuality and liberty, privacy must be protected, since

> [t]he man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.[13]

Cable companies can invade an individual's privacy in three different ways. First, privacy is invaded when cable companies compile data in an individually identifiable manner. Second, privacy is invaded when such information is disclosed to outside sources. Finally, privacy is invaded if interactive cable is used as a surveillance device. Each manner of privacy invasion is discussed below.

A. Compilation of Data in an Individually Identifiable Manner

Two-way systems may be a source of great enjoyment, allowing the viewer to actively participate in the programs offered. For example, the

---

11. Fried, *supra* note 8, at 483-84.

12. *See* United States v. United States Dist. Court, 407 U.S. 297, 314 (1972). The Court noted that:

> History abundantly documents the tendency of Government . . . to view with suspicion those who most fervently dispute its policies. . . . The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public disclosure, is essential to our free society.

13. Bloustein, *supra* note 10, at 1003.

Columbus QUBE system had a version of *The Gong Show* which enabled the viewers to press their buttons to eliminate acts.[14] Subscribers, however, are generally unaware that "the preferences they state, the products they select, the personal opinions they express can all be stored in the computer's memory and tallied, analyzed, and cross-referenced with demographic and financial information that is known about them."[15] People become concerned about threats to privacy only when they suffer some real harm. As a result, it is difficult to convince people that there is a threat until they see some "real horror stories."[16]

Absent any reported privacy violations from the compilation of data by cable companies,[17] only the potential for invasions of privacy can be examined. For instance, in order to take part in the shpping-at-home services, subscribers' names need to be recorded for mailing and billing purposes.[18] Consequently, the computer will know what each subscriber bought and how much he spent. Similarly, by using a cable company's banking-at-home services, the cable company's computer will be able to compile extensive financial data by keeping track of deposit and withdrawal transactions and to whom any money was sent.[19] Through the cable company's security system, the company can keep track of movements into and out of the house.[20] A cable company can also keep track of what subscribers are watching by monitoring their use of the pay-per-view services.[21] When answering public opinion or political questions, the computer can record how each subscriber responded.[22] Thus, the cable company is able to develop and maintain an accurate picture of the political, economic, and social activities of the subscriber.

There is concern that a cable company might release this information to the government, which could then use this information to create dossiers on these individuals.[23] Again, such abuse could tend to stifle dissent in the nation. Since it is a cable company and not the individual who would be controlling such personal information, the individual suffers a loss of privacy.

---

14. Wicklein, *supra* note 3, at 39.

15. *Id.*

16. *See Privacy Hearing*, *supra* note 6, at 2 (statement of Rep. Kindness). *See also* A.B.A. SECTION ON INDIVIDUAL RIGHTS AND RESPONSIBILITIES, REPORT ON THE NATIONAL SYMPOSIUM ON PERSONAL PRIVACY AND INFORMATION TECHNOLOGY 8 (1982).

17. *See* M. HAMBURG, ALL ABOUT CABLE, § 6.07[1], at 6-54 (1983).

18. Wicklein, *supra* note 3, at 40.

19. *See* Comment, *Cable Television Privacy Act: Protecting Privacy Interests from Emerging Cable TV Technology*, 35 FED. COM. L.J. 71, 78-79 (1983).

20. *See id.* at 79.

21. *See* Note, *Interactive Cable*, *supra* note 4, at 781.

22. *See id.* at 791.

23. For more information on dossiers in general, see A. WESTIN, PRIVACY AND FREEDOM 158-68 (1970). *See also* A. MILLER, *supra* note 9, at 39.

Because it is actually cheaper to store than to destroy information,[24] it is economically efficient to maintain such data longer than would be necessary for any originally intended business purpose. This increases the opportunity for a cable company to abuse this information. In order to reduce the opportunities for a cable company to abuse personal information, the companies should expunge such information after its intended business purpose has ceased. This would minimize the threat to individual privacy that exists because of the compilation of personal information.

B. Release of Personal Information to Outside Sources

Concern regarding the release of personal information is concomitant to the compilation of such information. The potential abuse of personal information vastly increases as a result of the "central storage and easy accessibility of computerized data."[25]

Abuse, for the purposes of this Note, can best be defined as the use of information for which it was not intended. Subscribers intend that the information a cable company compiles about them be used for the facilitation of services that the subscriber desires. If information is not used exclusively for this purpose, then such information is being abused. Examples of abuse would include situations where a cable company voluntarily releases personal subscriber data to the government, sells that information to businesses that want consumer data, or provides that information to political organizations which use the data for harrassing or fund-raising purposes. Since in each of these circumstances a subscriber loses control of personal information, subscriber privacy has been violated.

Suppose a cable company sold a list of the names of its subscribers who watched an X-rated movie to the Moral Majority, enabling the group to try to "save" those subscribers from "moral decay." This is objectionable, since the subscribers did not solicit such aid. A subscriber could have contacted the Moral Majority himself if he had wanted the group to know of his viewing habits. If the cable company had not sold this information to the Moral Majority, subscribers would not have been harrassed. Additionally, a subscriber loses control of personal information about himself—his viewing habits within the confines of his home. This may seem trivial to some, but

> [s]ome people feel emasculated when private information about them is disclosed or exchanged even though the data are accurate and they do not suffer any career or social damage. [T]hey think in terms of having

24. Linowes, *Must Personal Privacy Die in the Computer Age?*, 65 A.B.A. J. 1180, 1182 (1979).

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

> been embarrassed or demeaned by having been denuded of something that hitherto was theirs alone.[26]

This is true regardless of what information is released or to whom such information is released.

Currently, there have been no *known* instances of abuse of personal information maintained by cable companies.[27] But if the behavior of credit bureaus or banks is indicative, cable companies are also likely to misuse information available to them. Other record-keeping organizations willingly disclose information to third parties, absent any barriers to disclosure. For instance, approximately ninety-nine percent of all government requests directed at credit bureaus were granted, even if the request was made over the telephone and without notifying the subject of the request.[28] Likewise, absent barriers against the indiscriminant or unconsented to disclosure of information, cable companies could very well follow the path of other record-keeping organizations.

There have been *attempts* by third parties to obtain personal information maintained by cable companies. A few years ago in Columbus, Ohio, for instance, a movie theatre owner was being prosecuted for showing a sexually explicit movie in his theatre.[29] The same movie was also shown on the local cable system on a pay-per-view basis. The theatre owner tried to subpoena the cable company's records. He was seeking the names of all the viewers who had ordered the movie for the purpose of establishing the community's standards. He was actually seeking, however, to discover politically embarrassing information, that is, he was trying to find out if civic leaders, government officials, or the District Attorney had watched the movie. Fortunately, the court narrowed the subpoena to include only a request for the number of viewers of the program.[30] In this instance, the court eliminated the actual invasion of privacy by refusing to require the release of individually identifiable information. The *threat* to privacy was not eliminated, however, since the cable company could still have voluntarily complied with the original request. Unless restrictions are placed on cable companies regarding the release of personally identifiable information, the threat to privacy will continue.

---

26. A. MILLER, *supra* note 9, at 48-49 (footnote omitted).

27. M. HAMBURG, *supra* note 17, § 6.07[1], at 6-54. Just because there have been no abuses discovered does not mean that abuses of such information have not occurred.

28. Linowes, *supra* note 23, at 1182. For further details on how credit agencies operate, see Gonzales, *The Secret Life of Laurence Lorence*, PLAYBOY, June 1985, at 78.

29. Dionne, *Bill Seeks to Safeguard Cable Viewers' Privacy*, N.Y. Times, Jan. 12, 1982, at B3, col. 6.

30. *Id.*

C. CABLE TELEVISION AS A SURVEILLANCE DEVICE

Serious invasions of privacy would occur if cable television could be used as a surveillance device to monitor the subscriber's activities without his knowledge. The unauthorized viewing of and listening to our activities is an invasion of privacy, since the individual loses control of sensory information about himself. The thought of some other entity, whether it be a cable company or the government, watching and listening to the personal activities in one's home is extremely disturbing, especially if the device used to accomplish this is brought into the home by the subscriber himself. This type of invasion is particularly degrading since a "man whose home may be entered at the will of another, whose conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account."[31]

Though the threat to privacy would be very serious if cable television were used as a surveillance device, there is no evidence that interactive cable can presently be used in this way. This technology, however, may possibly exist.[32] Interactive cable systems are already able to monitor movements into and out of the subscriber's home as part of a security system some companies offer.[33] In addition, techniques to "listen in on" cable transmission, similar in concept to wiretapping telephone transmissions, are not "overly difficult,"[34] especially because cable systems provide less security than telephone systems.[35] Since cable television receives and transmits just like a telephone, it seems that cable can also be subjected to a form of wiretapping. It is not apparent, however, whether visual transmissions of activities in the subscriber's home can be relayed to the cable company in the same manner as a closed-circuit television system. Even if the technology has not yet been developed, the concern for potential privacy invasions exists nonetheless. As a result, the use of cable for surveillance purposes must also be considered when discussing the problems of threats to privacy by cable television.

---

31. Bloustein, *supra* note 10, at 973-74.

32. *See* Hodges, *Electronic Visual Surveillance and the Fourth Amendment: The Arrival of Big Brother?*, 3 HASTINGS CONST. L.Q. 261, 269 (1976) (describing the techniques of electronic surveillance on a videophone—a technology analogous to interactive cable).

33. Comment, *supra* note 19, at 79.

34. Ward, *Present and Probable CATV/Broadband-Communication Technology, app. A* to SLOAN COMMISSION ON CABLE COMMUNICATIONS, ON THE CABLE: THE TELEVISION OF ABUNDANCE at 211-12 (1971).

35. *Id.*

II. TORT REMEDIES FOR INVASIONS OF PRIVACY

If a cable subscriber's privacy has been invaded by the cable company, he could attempt to bring an action in tort for an invasion of privacy, assuming, of course, that the subscriber has become aware of the invasion. A private tort action, however, is an inadequate and undesirable method of protecting subscriber privacy.[36]

Originally, the common law did not recognize an action for an invasion of privacy. In 1890, the state of the law in the United States began to change when Samuel Warren and Louis Brandeis wrote one of the most influential law review articles in American jurisprudence, *The Right to Privacy*.[37] They characterized privacy as the right "to be let alone."[38] At first, courts were reluctant to adopt this theory, fearing it would open the floodgates on litigation.[39] But, beginning with the landmark case of *Pavesich v. New England Life Insurance Co.*[40] in 1905, courts began to recognize a right of privacy. Today, most American jurisdictions recognize the right of privacy, either judicially or legislatively.[41]

Seventy years after the Warren and Brandeis article, another influential privacy article was written by Dean Prosser.[42] He concluded that privacy was not one tort but four distinct torts which have nothing in common with each other except that they are all called privacy.[43] Prosser characterized the four torts as:

> 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> 2. Public disclosure of embarrassing private facts about the plaintiff.
>
> 3. Publicity which places the plaintiff in a false light in the public eye.
>
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[44]

The *Restatement (Second) of Torts* has incorporated Prosser's characterizations,[45] as have a number of states.[46]

---

36. *See infra* text accompanying notes 58-69.

37. Warren & Brandeis, 4 HARV. L. REV. 193 (1890).

38. *Id.* at 195 (quoting T. COOLEY THE LAW OF TORTS 29 (2d ed. 1888) .

39. *See, e.g.*, Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902).

40. 122 Ga. 190, 50 S.E. 68 (1905).

41. *See* Prosser, *Privacy*, 48 CALIF. L. REV. 383, 386-88 (1960).

42. *Id.*

43. *Id.* at 389.

44. *Id.*

45. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

46. *See, e.g.*, Diaz v. Oakland Tribune, Inc., 139 Cal. App. 118, 126, 188 Cal. Rptr. 762, 767-68 (1983).

At first glance, it is highly improbable that either the false light[47] or the appropriation[48] privacy actions are applicable here. But, it seems that the public disclosure and intrusion privacy actions may, on the surface, provide relief when a cable company invades a subscriber's privacy.

A. PUBLIC DISCLOSURE

On the surface, this form of privacy looks like it may apply when the cable company releases personal information to outside sources. But the tort of public disclosure requires that the information released be disclosed to the public.[49] The mere disclosure to a third party does not give rise to a cause of action.[50] So, for example, the release of personal credit information[51] or subscriber lists[52] to third parties and not

47. According to RESTATEMENT (SECOND) OF TORTS § 652E (1977):

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
>
> (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
>
> (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

The false light tort is difficult to apply to a cable company which invades its subscribers' privacy, since comment a requires the information to be made public. This privacy action fails to provide relief when a cable company only reveals information to the government, since this action does not fit the definition of publicity in § 652D comment a. Furthermore, § 652E comment a requires that the information that was made public be untrue. Presumably, a cable company, when revealing information in its files, would be revealing information that is true. For these reasons, it would be difficult to assert a false light claim in the cable context.

48. According to RESTATEMENT (SECOND) OF TORTS § 652C (1977), "[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy." In order for there to be an appropriation, the cable company must take for its own use or benefit the subscriber's "reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness." *Id.* § 652C comment c. It is unlikely that collecting or disclosing information, or conducting subscriber surveillance, will fall into this definition. As a result, it would be difficult to assert an appropriation privacy action.

49. Flowers v. Bank of Am. Nat'l Trust & Sav. Ass'n, 67 Or. App. 791, 797, 679 P.2d 1385, 1389 (1984). RESTATEMENT (SECOND) OF TORTS § 652D comment a (1977) states that the matter is made public "by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."

50. Vogel v. W. T. Grant Co., 458 Pa. 124, 132, 327 A.2d 133, 137 (1974) (merely revealing the information to the plaintiff's mother and to the plaintiff's employer did not constitute a public disclosure). RESTATEMENT (SECOND) OF TORTS § 652D comment a (1977) states that "it is not an invasion of privacy . . . to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons."

51. Tureen v. Equifax, Inc., 571 F.2d 411, 417-19 (8th Cir. 1978).

52. Tobin v. Civil Serv. Comm'n, 416 Mich. 661, 673, 331 N.W.2d 184, 189-90 (1982).

to the general public is not actionable under this tort. Likewise, no cause of action would arise if the cable company merely releases similar types of personal information to a business, the government, or a political organization without also releasing it to the general public. In such a situation, the subscriber may be left without a remedy.

B. INTRUSION

If a cable television is used as a surveillance device without the knowledge or consent of the subscriber, it will most likely be found to be an actionable invasion of privacy analogous to the eavesdropping and wiretapping cases. The cases generally hold that these methods of surveillance constitute an invasion of privacy under the intrusion tort.[53] One case even goes so far as to say that the mere existence of a surveillance device in the home is enough to establish a cause of action, even absent any proof that conversations were overheard.[54] Consequently, a court would probably hold that the use of cable television as a surveillance device is an actionable invasion of privacy, since visual surveillance is conceptually similar to aural surveillance.

It is highly unlikely, however, that the mere compilation of data is actionable under this privacy action. Most courts recognize that the mere gathering of information about a particular individual does not give rise to a cause of action under intrusion.[55] In order to be actionable, the gathering of information must be through "improperly intrusive means."[56] There would probably be no violation if the collection of information was relevant to a legitimate business purpose.[57] Because a cable company may be able to show that their maintenance of personal information is necessary for legitimate business purposes, it would be unlikely that a subscriber would succeed if he brought an action alleging intrusion merely through the compilation of personal data.

The court goes on to say in *Tobin* that "[n]o other jurisdiction has ever recognized a cause of action based on the release of an individual's name and address without more." *Id.* at 675, 331 N.W.2d at 190 (footnote omitted). *See also* Annot., 82 A.L.R.3d 772 (1978).

53. *See, e.g.*, McDaniel v. Atlanta Coca-Cola Bottling Co., 60 Ga. App. 92, 2 S.E.2d 810 (1939) (microphone in a hospital room); Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931) (wiretap on a telephone); Hamberger v. Eastman, 106 N.H. 107, 206 A.2d 239 (1964) (listening device in plaintiff's bedroom).

54. Hamberger v. Eastman, 106 N.H. 107, 111-12, 206 A.2d 239, 241-42 (1964).

55. *See, e.g.*, Peacock v. Retail Credit Co., 302 F. Supp. 418, 423 (N.D. Ga. 1969), *aff'd*, 429 F.2d 31 (5th Cir. 1970), *cert. denied*, 401 U.S. 938 (1971); Nader v. General Motors Corp., 25 N.Y.2d 560, 566-67, 307 N.Y.S.2d 647, 652-53, 255 N.E.2d 765, 768-69 (1970) (applying District of Columbia law).

56. Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969).

57. *See* Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978).

C. RELIANCE ON THE TORT TO PROTECT CABLE PRIVACY IS INADEQUATE AND UNDESIRABLE

Numerous problems arise if the various privacy torts are relied upon to protect subscribers against invasions of privacy.

1. *Inadequacy of the Remedy*

a. *Prosser's characterizations are unlikely to be expanded*: One major problem with relying on the tort of privacy is that courts are reluctant to expand the tort beyond Prosser's characterizations. Some courts take the view with privacy law *only* protects Prosser's four areas. Courts have held that if the invasion does not fit into one of the four categories, then there is a failure to state a cause of action.[58] These courts fail to recognize that one's human dignity may be damaged by many types of invasions which were not recognized by Prosser, especially because many new intrusive technologies have been developed since he wrote his article in 1960. As a result of this reluctance to expand the privacy categories, it is unlikely that courts will expand the privacy torts into areas invaded by the cable company which do not fit into any category previously established. As a result, unless the privacy actions are expanded, a subscriber may be left without an effective remedy.

b. *Consent doctrine*: The consent doctrine poses another major problem in relying on tort to protect against invasions of privacy. Basically, the doctrine states that there is no actionable invasion of privacy if the subscriber consented to the invasion.[59] The subscriber may consent either expressly or impliedly.[60] If the invasion, however, goes beyond the consent that was granted, the invasion would be actionable.[61]

Express consent will probably be stated in the subscriber's cable contract, and its scope will be relatively easy to determine. The scope of

---

58. See, e.g., Nader v. General Motors Corp., 25 N.Y.2d 560, 565-71, 307 N.Y.S.2d 647, 651-56, 255 N.E.2d 765, 770-71 (1970), where the court held that since some of the defendant's allegations fit into none of the categories, there was no invasion of privacy as to those allegations. The concurring justice criticizes the majority opinion stating:

> True, scholars, in trying to define the elusive concept of the right of privacy, have, as of the present, subdivided the common law right into separate classifications, most significantly distinguishing between unreasonable intrusion and unreasonable publicity. This does not mean, however, that the classifications are either frozen or exhausted, or that several of the classifications may not overlap.

Id. at 572, 307 N.Y.S.2d at 657, 255 N.E.2d at 772 (Breitel, J., concurring in result) (citations omitted).

59. Volk v. Auto-Dine Corp., 177 N.W.2d 525, 529 (N.D. 1970).

60. Anderson v. Low Rent Hous. Comm'n, 304 N.W.2d 239, 249 (Iowa), *cert. denied*, 454 U.S. 1086 (1981).

61. RESTATEMENT (SECOND) OF TORTS § 892A(2)(b), (4) (1977).

implied consent, however, may be difficult to determine. The subscriber may have impliedly consented to the compilation of data for business purposes by taking part in the interactive services, since he probably knows that records must be compiled to complete the transactions. It is not clear, however, whether or not he has consented to the release of such information to outside sources. If the subscriber is aware of the compilation and release of data and continues to use the services, he may be held to have consented to the invasion, since an implied consent may be determined from the subscriber's conduct.[62] A subscriber who continues to use the cable services even though he knows that his transactions are being revealed to outside sources would probably be held to have given an implied consent to the continued release of that information.[63] Similarly, if cable television could be used as a surveillance device and the subscriber is aware of this capability and allows its continued presence in his home, he may be held to have impliedly consented to continued surveillance.[64] Thus, if a subscriber allows the cable system into his home and he knows of the system's capabilities, an invasion of privacy tort remedy may not be available to the subscriber. An additional problem arises as to when such knowledge will be imputed to the subscriber if he did not have knowledge in fact.

If, however, limited consent is given and the invasion goes beyond the consent granted, then the cable company may be liable for the actions which go beyond the consent granted, especially if the capabilities of invading privacy were unknown to the public.[65] Because of the many gray areas in this doctrine, courts may be inconsistent in handling these problems. As a result, the tort remedy would not provide as much protection as necessary.

2. *Undesirability of the Remedy*

Even if the tort remedy were adequate to protect against invasions of privacy by a cable company, there are a number of reasons why it is undesirable as a remedy. First, not all states recognize a right to privacy in areas that could serve as protections against cable invasions.[66] As a result, subscribers in states that do not recognize this cause of ac-

62. *See* 62 AM. JUR. 2D *Privacy* § 18, at 703 (1972).

63. *See* State v. Johnson, 52 Or. App. 651, 654, 628 P.2d 789, 791 (1981) (silence or inaction may constitute consent to certain conduct).

64. *See* Rawls v. Conde Nast Publications, Inc., 446 F.2d 313, 317 (5th Cir. 1971), *cert. denied*, 404 U.S. 1038 (1972) (since the plaintiff acquiesced to the continued presence of the defendant's employees in her home at the time of the alleged invasion of privacy, she impliedly consented to the invasion).

65. *See* RESTATEMENT (SECOND) OF TORTS § 892A(4) comment h (1977).

66. *See, e.g.*, Evans v. Sturgill, 430 F. Supp. 1209, 1213 (W.D. Va. 1977) (no general right of privacy exists in Virginia).

tion have no tort remedies to protect their privacy rights. Second, a subscriber may be reluctant to bring a suit, as he may not want more people to be privy to his personal matters.[67] By allowing only this remedy for him, we may be requiring a subscriber to incur additional privacy losses in order to go to court. Third, a subscriber may also be reluctant to bring a suit since the litigation costs may outweigh the potential amount of recoverable damages.[68] A court, in fact, may be willing to award only nominal damages absent a showing of special damages, as in defamation cases. Finally, plaintiffs in privacy suits are seldom successful.[69] Since a loss of privacy is an intangible injury, unlike physical or pecuniary injuries, it is often difficult to persuade a jury that an injury has in fact occurred.

For these reasons, it is undesirable to rely on tort law to remedy invasions of privacy. Therefore, a cable subscriber must be protected against invasions of privacy through other means.

III. CONSTITUTIONAL PROTECTIONS OF PRIVACY

The next inquiry is to determine whether the U.S. Constitution protects subscriber privacy from intrusions either by a cable company or by the government. A cable company would be limited by the Constitution only if a cable company's actions constitute state action.[70] Courts have struggled with the determination of whether particular conduct is private or state action.[71] The established principle is that state action will be found "in the exercise by a private entity of powers traditionally exclusively reserved to the state."[72]

There are two cases which make it unlikely that actions of a cable company would constitute state action. The first, *Jackson v. Metropolitan Edision Co.*,[73] is a Supreme Court case. The entity in question was an electric company. It was urged that the electric company's action be considered public, since the utility was a monopoly and was heavily regulated. The Court held that

> [t]he mere fact that a business is subject to state regulation does not by itself convert its action into that of the State . . . . Nor does the fact that the regulation is extensive and detailed . . . do so. [T]he inquiry must be whether there is a sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of

67. A. MILLER, *supra* note 9, at 188.

68. Comment, *supra* note 19, at 81. *See also* A. MILLER, *supra* note 9, at 188.

69. *See* A. MILLER, *supra* note 9, at 188.

70. *See* The Civil Rights Cases, 109 U.S. 3, 11 (1883).

71. *See, e.g.*, Columbia Broadcasting Sys. v. Democratic Nat'l Comm., 412 U.S. 94 (1973).

72. Jackson v. Metropolitan Edison Co., 419 U.S. 345, 352 (1974).

73. *Id.*

the latter may be fairly treated as that of the State itself.[74]

In addition, the Court held that the "fact [that the operation is a state created monopoly] is not determinative in considering whether [its actions are] 'state action[s]'. . . ."[75]

The Court decided that providing electricity was an activity not traditionally reserved to the state. Since there was not a sufficient nexus between the state and the discontinuance of the petitioner's electricity, the Court held that there was no state action. Because a cable company is not nearly as heavily regulated as an electric company, and because the delivery of cable services is not traditionally a function of government, it is unlikely that a cable company's actions would be found to constitute state action.

This result was reached in an Eighth Circuit case, *Movie Systems, Inc. v. Heller*.[76] In this case, the cable company used electronic equipment installed in a van to detect signals from Heller's microwave antenna in order to determine whether he was intercepting cable programming. The court held that there were no "facts which would support a finding of state action."[77] As a result, Heller's constitutional claim against Movie Systems was barred. Heller was also unable to raise a state tort action, since Minnesota had never recognized a cause of action for an invasion of privacy.[78] Thus, at least one circuit has held that actions by a cable company do not constitute state action. But because the Supreme Court has never determined whether actions by a cable company constitute state action, the issue may still be undecided.

Without a finding of state action, the Constitution would not prevent cable companies from compiling and disclosing personal information about a subscriber or prevent surveillance of the subscriber's home. The government, however, would be bound by constitutional restraints in trying to obtain information from a cable company or in setting up its own surveillance system. For the purpose of the constitutional analysis, this Note assumes that the requisite state action can be found in the actions of a cable company.

Generally, there are two types of constitutionally based privacy—fourth amendment privacy and fourteenth amendment/substantive due process privacy—which may be applicable in the cable television context. These two privacies differ and must be viewed separately.

---

74. *Id.* at 350-51 (citations omitted).

75. *Id.* at 351-52.

76. 710 F.2d 492 (8th Cir. 1983).

77. *Id.* at 496.

78. *Id.*

A. FOURTH AMENDMENT PRIVACY

The fourth amendment of the U.S. Constitution states that people have the right "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[79] The government must obtain a search warrant to search an area where a person has an actual expectation of privacy.[80] But if a person knowingly exposes something to the public, it has been held that the person did not have a reasonable expectation of privacy in that area.[81] The fourth amendment applies not only to the search and seizure of tangible items, but also to government surveillance.[82]

An important fourth amendment case, *United States v. Miller*,[83] may apply to cable television. In *Miller*, the government went to Miller's bank to look at the records the bank kept on Miller's financial transactions. The records included copies of each check that Miller had written. The bank allowed the government to inspect the records, not with a search warrant, but with an allegedly defective subpoena duces tecum served upon the bank. The bank never notified Miller of the subpoena. Subsequently, the government used information obtained from the bank records to convict Miller of a tax conspiracy in liquor bootlegging. The Supreme Court held that Miller had no standing to challenge the validity of the subpoena, reasoning that the records were not Miller's private papers because they belonged to the bank.[84] The Court also held that there was "no legitimate 'expectation of privacy' in their contents" because the records contained only "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[85] The Court found that a depositor takes the risk that the bank will reveal that information to the government.[86] The Court stated that the fourth amendment

> does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[87]

Accordingly, the government was held not to have violated Miller's fourth amendment rights.

---

79. U.S. CONST. amend. IV.
80. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
81. *Id.* at 351.
82. *See* United States v. United States Dist. Court, 407 U.S. 297, 313 (1972).
83. 425 U.S. 435 (1976).
84. *Id.* at 440.
85. *Id.* at 442.
86. *Id.* at 443.
87. *Id.* (citations omitted).

Relying on the California Supreme Court case *Burrows v. Superior Court*,[88] the dissent pointed out that a depositor *does* have a reasonable expectation that his bank records will remain private.[89] The dissent was concerned that the majority would allow the bank—a neutral entity—to consent to the invasion of privacy of one of its depositors, especially without notifying the depositor of the invasion.[90] The dissent felt that bank customers should be afforded great protection, since checking accounts are essential for participation in the modern economic system, and thus not a truly voluntary relinquishment of an expectation of privacy.[91]

Miller is particularly applicable to the area of cable television because many of the records maintained by cable companies are similar to records maintained by the bank in *Miller*. Applying the *Miller* rationale, a subscriber would have no reasonable expectation of privacy because he voluntarily reveals his transactions to the cable company. A subscriber must take the risk that the cable company might reveal his personal information to the government. Since, under *Miller*, there would be no reasonable expectation of privacy, a search of the subscriber's records could be conducted without a warrant. Unless a cable company objects, the government would be able to go through each subscriber's file, gather information, and create its own files on individuals. This could all occur without the subscriber's knowledge.

The *Miller* decision has evoked both congressional and state judicial responses. Congress rejected the premise of the *Miller* holding by recognizing a reasonable expectation of privacy in bank records in the Right to Financial Privacy Act.[92] The Act, however, does not apply to records maintained by a cable company.[93] Thus, the *Miller* rationale is still applicable to cable records, at least on the federal level.

A number of state courts have rejected *Miller*, basing their decisions on their own state constitutions, and have granted depositors an expectation of privacy in their bank records.[94] The rationales of these

88. 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974). The continued validity of *Burrows* is in doubt after the California Supreme Court's decision in *In re* Lance W., 37 Cal. 3d 873, 694 P.2d 744, 210 Cal. Rptr. 631 (1985) (holding that Proposition 8 requires evidence to be admitted, unless exclusion is mandated by the federal constitution).

89. *Miller*, 425 U.S. at 448 (Brennan, J., dissenting).

90. *Id.* at 450.

91. *Id.* at 451.

92. 12 U.S.C. §§ 3401-3422 (1982).

93. For a further discussion as to the inapplicabilty of the Act, see *infra* text accompanying notes 124-31.

94. *See, e.g.*, Charnes v. DiGiacomo, 200 Colo. 94, 612 P.2d 1117 (1980); People v. Jackson, 116 Ill. App. 3d 430, 452 N.E. 2d 85 (1983); Suburban Trust Co. v. Waller, 44 Md. App. 335, 408 A.2d 758 (1979); Commonwealth v. DeJohn, 486 Pa. 32, 403 A.2d 1283 (1979) *cert. denied*, 444 U.S. 1032 (1980).

cases, however, will probably not be applied to cable records. These courts were persuaded by *Burrows* and the dissent in *Miller* when reaching their decisions, reasoning that a checking account was almost essential for participation in the modern economic system. Cable television, on the other hand, is not as widespread or as essential for participation in the economic system. Cable television is still in its infancy and may be viewed as a luxury. A court may decide that the use of cable at the present time is truly voluntary and may be reluctant to extend the rationale of these cases to cable records. Thus, cable records would be unprotected under the fourth amendment and under similar state constitutional provisions.

B. FOURTEENTH AMENDMENT/SUBSTANTIVE DUE PROCESS PRIVACY

The Supreme Court has never explicitly recognized a general right of privacy that is protected by the Constitution.[95] Since *Griswold*, however, the Court has held that some types of privacy are protected by the Constitution. Therefore, it must be determined whether a right not to have personal data disclosed or compiled, that is, informational privacy, is one recognized by the Supreme Court as a protected privacy under the Constitution.

Informational privacy is necessary in a society which values individual liberty.[96] *Whalen v. Roe*[97] is the most important case to discuss informational privacy. *Whalen* involved a state law which authorized the state to record the names and addresses of all patients who received prescriptions for certain drugs in a centralized computer file. The state obtained the information from doctors who prescribed the drugs and who were required to supply the information to the state. The Supreme Court unanimously rejected the attack on the information system. The Court stated, however, that two types of privacy exist rather than just one—"[o]ne is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[98] These have been characterized as the confidentiality and autonomy branches of privacy.[99] The Court held that the state law did not pose a sufficiently grievous threat to either branch of privacy.[100] The Court also implied that because mechanisms which prohibited the unwarranted disclosures of data were available,

95. *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973); Eisenstadt v. Baird, 405 U.S. 438 (1972); Griswold v. Connecticut, 381 U.S. 479 (1965).

96. *See supra* text accompanying notes 8-13.

97. 429 U.S. 589 (1977).

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

99. *See* Plante v. Gonzales, 575 F.2d 1119, 1127-37 (5th Cir. 1978), *cert. denied*, 439 U.S. 1129 (1979).

100. *Whalen*, 429 U.S. at 600.

the system had shown some concern with an individual's right of privacy.[101] Because no unwarranted disclosures occurred, the Court reserved the question of whether the "unwarranted disclosure of accumulated private data" was a violation of the right of privacy.[102] Thus, the accumulation of data in itself appears not to violate the Constitution, at least where adequate safeguards against unwarranted disclosures are available. The Court, however, did not state what constitutes adequate safeguards. Because cable companies and the system involved in *Whalen* both maintain records which contain personally identifiable information, the mere accumulation of data by a cable company probably would not violate a constitutional right of privacy. Thus, the Constitution probably does not offer protection against the mere compilation of data.

The holding in *Whalen* did not address the issue of disclosure. The majority opinion in dicta did state, however, that the Constitution protects an individual's interest in not having personal matters disclosed.[103] The Court was aware "of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks"[104] and conceded that the duty of nondisclosure "in some circumstances . . . has its roots in the Constitution."[105] The majority, however, never defined the situations where the duty of nondisclosure would be rooted in the Constitution.

The concurring opinions in *Whalen* make it difficult to predict how the Court would handle a disclosure case. Justice Brennan, in his concurrence, believed that the broad dissemination of personal information would implicate constitutionally protected privacy rights.[106] In a separate concurrence, Justice Stewart disagreed, stating that no such constitutional right exists, and no cases support Brennan's assertion.[107] Because the Court's position as to the right to nondisclosure was unclear, the lower courts have split as to whether a right not to have personal information disclosed exists.[108]

---

101. *See id.* at 605.

102. *Id.* at 605-06.

103. *Id.* at 599.

104. *Id.* at 605.

105. *Id.*

106. *Id.* at 606 (Brennan, J., concurring).

107. *Id.* at 608-09 (Stewart, J., concurring).

108. For lower court decisions which hold that there is a constitutional right in not having personal information disclosed, see Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981); United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980). For a lower court decision which holds that there is no constitutional right in not having personal information disclosed, see J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981). For a criticism of the *DeSanti* case, see Case Comment, *A Constitutional Right to Avoid Disclosure of Personal Matter: Perfect Privacy Analysis in* J.P. v. DeSanti, 71 GEO. L.J. 219 (1982).

Even if a constitutional right not to have personal information disclosed exists, the Court in *Whalen* did not clearly state the standard of review to be used for a disclosure case. The lower courts have generally used a balancing test in disclosure cases, unlike the strict scrutiny used in the autonomy cases.[109] In justifying its use of the lower standard, one lower court has stated that it "seems in keeping both with the Supreme Court's reluctance to recognize new fundamental interests requiring a high degree of scrutiny for alleged infringements, and the Court's recognition that some form of scrutiny beyond rational relation is necessary to safeguard the confidentiality interest."[110] One commentator, however, has stated that the reason for the lower standard was that to apply "that stringent standard [strict scrutiny] to the confidentiality right would unduly hinder the government's legitimate and necessary use of information."[111] Whatever the reason for the lower standard, it is clear that the courts which recognize the right not to have personal information disclosed use the balancing test.

The courts balance the privacy interests of the individual against the societal interest in the disclosure.[112] The court in *United States v. Westinghouse Electric Corp.* listed a number of factors to be considered when engaging in "the delicate task of weighing competing interests."[113] The factors the court took into account were: (1) the type of record requested; (2) the information that the record may contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosures; (6) the degree of the need for access to the records; and (7) whether some statute, express policy, or public interest favors access.[114] Even after considering these factors, the court in *Westinghouse Electric* still allowed the disclosure of the employees' medical records.[115] It is possible, however, that after taking into account each of these factors, a court may still allow a cable company to disclose its

109. *See, e.g.*, Barry v. City of New York, 712 F.2d 1554 (2d Cir.), *cert. denied*, 464 U.S. 1017 (1983).

110. *Id.* at 1559.

111. Note, *The Constitutional Right to Confidentiality*, 51 GEO. WASH. L. REV. 133, 143 (1982).

112. *See, e.g.*, United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).

113. *Id.*

114. *Id.*

115. The court conditioned the release of the medical records on the government agency's notification of the employees. *Id.* at 581. This allowed each employee to raise a personal claim of privacy.

records without requiring notification to the subscribers.[116]

There are problems with relying on the Constitution to protect disclosure rights, that is, if such rights exist. The only way a cable subscriber could keep his records from being disclosed is to show that his privacy interests are greater than society's interest in the information. This is more troublesome than in the tort area, since the subscriber would have to go to court to show why his interests are worth protecting—thus losing privacy in the process, especially if the court must consider the type of information which may be contained in the records in order to make a decision. Thus, it is undesirable to rely on the fourteenth amendment for protection against unwarranted disclosures.

IV. STATUTORY PRIVACY PROTECTIONS

A. NON-CABLE STATUTES DEALING WITH PRIVACY

There are a number of federal statutes which deal with some of the privacy problems in a non-cable context. It must be determined whether any of these statutes provide protection from an invasion of privacy by a cable company.

1. *Privacy Act of 1974*

The Privacy Act of 1974[117] is probably the most comprehensive piece of privacy legislation ever enacted. The Act provides that an agency may not disclose any information about an individual—either to another agency or another individual—without the individual's written consent.[118] Each agency must also allow any individual access to his records or to any information pertaining to him upon his request.[119] The individual has an opportunity to correct any erroneous information about himself.[120] Finally, an agency may only maintain such information which is "relevant and necessary" to the accomplishment of a purpose of the agency.[121]

The Privacy Act, however, only applies to government *agencies*.[122] A cable company does not fit the statute's definition of an agency.[123] As a result, the protections found in the Privacy Act do not apply to cable

116. This could occur if a court believed that subscribers voluntarily gave the information to the cable company, thus vitiating any privacy interest.

117. 5 U.S.C. § 552a (1982).

118. *Id.* § 552a(b).

119. *Id.* § 552a(d)(1).

120. *Id.* § 552a(d)(2).

121. *Id.* § 552a(e)(1).

122. For instance, § 552a(b) says "No agency shall disclose . . .," not "No entity shall disclose . . . ."

123. *See id.* § 552(e).

companies. Thus, the Privacy Act would not provide protection to a cable subscriber against a cable company.

2. *Right to Financial Privacy Act of 1978*

The Right to Financial Privacy Act of 1978[124] was enacted in response to the decision of *United States v. Miller*.[125] The Right to Financial Privacy Act provides that no government authority[126] may have access to or obtain copies of any individual's financial records, unless the individual authorizes such a disclosure, the records are subpoenaed, or the records are subjected to a search warrant.[127] Further, a financial institution may not provide such information if the government authority has not followed the requirements set out in the statute.[128] In addition, a financial institution cannot require that an individual authorize disclosures as a condition for doing business.[129]

Because a cable company keeps the financial and banking data of its subscribers which use those services, it would appear that the Right to Financial Privacy Act would be applicable. The Act, however, does not apply to those financial records held by cable companies. The Act applies only to records held by financial institutions.[130] A financial institution under the Act is a bank, savings and loan, card issuer, trust company, credit union, or similar entity.[131] Because a cable company is not an institution listed under the Act, it would not be prevented from voluntarily granting a government agency access to a subscriber's financial records.

3. *Wiretap Control Legislation*

Under 18 U.S.C. § 2511(1), any person who willfully intercepts a wire or oral communication may be fined up to $10,000 and be imprisoned for up to five years. An oral communication is defined as any "oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception."[132] Clearly, if a cable company listens in on a subscriber's conversations, then a violation under section 2511(1) occurs.

---

124. 12 U.S.C. §§ 3401-3422 (1982).

125. *See supra* text accompanying note 92.

126. "Government authority" is defined as "any agency or department of the United States, or any officer, employee, or agent thereof." 12 U.S.C. § 3401(3) (1982).

127. *Id.* § 3402.

128. *Id.* § 3403.

129. *Id.* § 3404(b).

130. For instance, § 3402 refers to "financial records of any customer from a financial institution, " not "financial records of any customer from any entity."

131. *Id.* § 3401(1).

132. 18 U.S.C. § 2510(2) (1982).

If a cable company's surveillance is visual rather than aural, a more difficult situation arises, since visual surveillance does not fit the definition of "oral communication." Section 2511(1) prohibits the willful interception of any wire or oral communication or anyone who uses a device to intercept such communications. But, section 2510(4) defines "intercept" as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[133] Thus, the statute does not prohibit the visual interception of the contents of any wire or oral communication, enabling a company to conduct visual surveillance whether or not a cable system constitutes "wire communication."[134] As a result, this statute, as with the Privacy Act and the Right to Financial Privacy Act, would not offer protection to cable subscribers against invasions of privacy by a cable company.

B. CABLE PRIVACY STATUTES

Because the above laws protecting privacy may not offer much protection to cable subscribers, some legislatures have enacted privacy laws specifically to protect cable subscribers.

1. *State Statutes*

a. *Illinois*: The first state to pass a cable privacy act was Illinois in 1981.[135] The Illinois law prohibits the surveillance, both aural and visual, by cable companies of its subscribers without the knowledge or permission of the individual subscriber.[136] The law also prohibits the disclosure of subscribers' names and addresses to both public and private organizations without notice to the subscribers.[137] The disclosure of subscriber viewing habits without the subscriber's consent is also prohibited.[138]

The statute, however, is deficient in several respects. First, the compilation of individually identifiable data is not prohibited, nor is it even regulated. Second, if the goal is to maximize an individual's control of information about himself, then the law should require the subscriber's express written consent *before* there is any disclosure, since, as noted earlier, a number of problems arise if implied consent is al-

133. *Id.* § 2510(4).

134. It has been held that television and photographic surveillance does not fall within the ambit of the wiretapping statute. *See* United States v. Torres, 751 F.2d 875, 880 (7th Cir. 1984), *cert. denied*, 105 S. Ct. 1853 (1985) (television surveillance); Sponick v. City of Detroit Police Dep't, 49 Mich. App. 162, 198, 211 N.W.2d 674, 690 (1973) (photographic surveillance).

135. ILL. ANN. STAT. ch. 38, §§ 87-1 to -3 (Smith-Hurd 1985).

136. *Id.* § 87-3(a)(1).

137. *Id.* § 87-3(a)(2).

138. *Id.* § 87-3(a)(3).

lowed.[139] The Illinois law thus provides some protection, but not enough.

b. *California*: The most comprehensive state cable privacy statute was passed by California in 1982.[140] The California law prohibits the surveillance of the subscriber without his express written consent.[141] The law also prohibits the disclosure of individually identifiable information without the subscriber's express written consent.[142] Data may be compiled, but "only to the extent reasonably necessary for billing purposes and internal business practices," while the company is required to "maintain adequate safeguards" to ensure the confidentiality of that information.[143] Individually identifiable information cannot be made available to government agencies absent "legal compulsion"; however, the cable company must notify the subscriber when an agency seeks the information.[144] In addition, a subscriber has the right to inspect any information maintained on him and has the right to correct any errors.[145] Finally, localities are not pre-empted from enacting even more stringent privacy laws on cable franchises.[146]

The California law maximizes subscriber privacy by granting the subscriber a great deal of control regarding personal information. It guarantees him the right to know what information is maintained on him. While the law recognizes that cable companies have a legitimate need to maintain subscriber information, it regulates the use of such information. One flaw in the California law, however, is that it does not require the destruction of information after the need for such information has passed. Nevertheless, the California law does provide substantially more privacy protection than the Illinois law.

2. *Federal Law*

A section on cable subscriber privacy was included in the Cable Communications Policy Act of 1984.[147] The Act prohibits the collection of individually identifiable information without the express consent of the subscriber, unless the data is necessary to render a cable service.[148]

---

139. *See supra* text accompanying notes 59-65.

140. CAL. PENAL CODE § 637.5 (Deering 1983).

141. *Id.* § 637.5(a)(1).

142. *Id.* § 637.5(a)(2).

143. *Id.* § 637.5(b).

144. *Id.* § 637.5(c).

145. *Id.* § 637.5(d).

146. *Id.* § 637.5(*l*).

147. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 2, 1984 U.S. CODE CONG & ADMIN. NEWS (98 Stat.) 2779, 2794 (codified at 47 U.S.C. § 551 (Supp. II 1985)).

148. 47 U.S.C. § 551(b) (Supp. II 1985).

Disclosure of personal information is not permitted without the express consent of the subscriber, unless it is necessary to render a cable service or to comply with a court order.[149] A subscriber has the right to remove his name and address from a list that the cable company may reveal to outside sources[150] and is entitled to have access to his files.[151] Finally, the cable company must destroy any individually identifiable information after that information has served the purpose for which it was collected.[152]

The Act requires express consent *before* the invasion of privacy occurs (similar to the California law), thus maximizing subscriber privacy. The Act, however, affords more protection than the California law, since it provides for the destruction of data which has outlived its originally intended purpose. The Act, however, does not protect subscribers from surveillance by the cable company. Nevertheless, the subscriber privacy section of the Cable Communucations Policy Act offers a great deal of privacy protection.

V. PROPOSALS

A. FEDERAL CABLE PRIVACY STATUTE

Statutes which explicitly protect individuals from privacy invasions by cable companies offer the best protections for subscribers of cable television. To fully protect the subscribers' privacy, a federal law, rather than a state or local law, must be enacted. If the states were left to develop such policies, "[p]atchwork legislation and confusion" would ensue.[153] Interactive cable allows subscribers to bank, shop, and carry on other activities between states. This can lead to some problems. For example, a subscriber living in California could order clothes from a company in Illinois. Thus, information could be maintained in a state different than that of the subscriber's residence. In addition, a single company may have franchises in more than one state. These franchised companies could be severely hampered by conflicting and inconsistent state laws. Therefore, to avoid inconsistent state laws, a comprehensive federal cable privacy law is necessary.

The recently adopted Cable Communications Policy Act regulates the privacy of cable subscribers.[154] A number of amendments, however, are needed in order to offer greater privacy protection for the cable subscriber. First, as noted above, aural and visual surveillance by the cable

149. *Id.* § 551(c).
150. *Id.* § 551(c)(2)(C)(i).
151. *Id.* § 551(d).
152. *Id.* § 551(e).
153. Linowes, *supra* note 24, at 1184.
154. *See supra* text accompanying notes 147-52.

company should be prohibited. Second, a cable company should be precluded from requiring consent as a precondition of receiving services.[155] If a cable company were allowed to require consent before cable services are provided, any legal protection would effectively be eliminated through the consent doctrine due to the monopoly advantage a cable company possesses. Finally, a cable company should not be allowed to charge higher rates to subscribers who do not give their consent, since this may also eliminate the law's protection through a form of extortion. It seems patently unfair to require a subscriber to pay an extra fee in order to receive the full protection of the law.

There are, however, two arguments against tough cable privacy laws. The first argument is that people trade off privacy invasions for the conveniences of cable.[156] This argument is flawed, however, in that most people are probably not aware that threats to privacy exist.[157] If people are not aware of these threats, then it cannot be said that they have affirmatively accepted these invasions. In fact, eighty-three percent of the public favors laws which would prohibit businesses and organizations which collect information from violating an individual's privacy.[158] In addition, it has been said that people will not be aware of the potential privacy threats unless "something tragic . . . happen[s], some national scandal that attracts the nation's attention."[159] Unless such a revelation occurs, people will remain unaware of the threats to their privacy.

In essence, the new federal cable legislation is a preventative measure. It was unusual that Congress, in passing the Act, was trying to avert a "national tragedy," rather than reacting to it after the fact.[160] Congress may have averted such a national tragedy. As a consequence, the public probably never became aware of some of the possible threats to privacy. The purpose of these amendments is to eliminate any holes in the Act, so that the public would not have to be exposed to any further threats to their privacy by cable companies.

The second argument against tough cable laws is that if the industry is excessively regulated, the full development of any new cable technology would be discouraged.[161] Although this is a strong argument, it

155. This provision would be similar to the provision found at 12 U.S.C. § 3404(b) (1982).

156. *See* Quade, *Privacy in Peril*, 69 A.B.A. J. 565, 567 (1983). *See also* K. GREENAWALT, *supra* note 9, at 42.

157. *See* A. WESTIN, *supra* note 23, at 160 (government dossiers).

158. *Privacy Hearing*, *supra* note 6, at 6 (statement of Louis Harris).

159. Quade, *supra* note 156, at 569.

160. *See Privacy Hearing*, *supra* note 6, at 89 (statement of Rep. English) ("We're not known to react until the fire is just about to consume the house.").

161. *See id.* at 78 (statement of Jean Handley, Vice-President, Personnel and Corpo-

is not persuasive against all tough privacy laws. Nevertheless, the legitimacy of this concern dictates that any privacy law must be sensitive to the continued development of the industry. A balance must exist between the maximization of subscriber privacy and the needs of the industry. The federal law shows such a concern and strikes the proper balance. The federal law does not prohibit the collection or dissemination of information. Rather, the federal law merely prohibits any *unauthorized* and *nonconsensual* collection or dissemination. Privacy is maximized by giving the subscriber control of the information about himself. The cable company's use of the information remains unrestricted so long as the subscriber is notified and grants permission for its use. The requirement does not seem to unduly hamper the cable companies. Similarly, the proposed amendments are also not unduly burdensome to the cable companies. Because a federal cable privacy law is the preferred method of protecting subscriber privacy, and because the proposed amendments will not stifle the development of new technologies, these proposed amendments to the Cable Communications Policy Act should be adopted.

B. FEDERAL PRIVACY PROTECTION AGENCY

In conjunction with a federal law regulating the privacy of cable subscribers, a federal privacy protection agency is necessary for complete subscriber privacy protection. Such an agency would serve two functions. First, the agency would have the responsibility of enacting new privacy regulations in response to new developments in cable technology. It is important that such a function be left with an agency rather than with Congress. It has been said that "while technology races, legislation crawls."[162] It has also been said that "the vast majority of congressmen have little or no comprehension of the new information technologies, much less their broader societal implications."[163] If this is true, then an organization composed of experts in the field—familiar with cable technology and its inherent problems—is necessary to develop new rules as the technology becomes more sophisticated. In addition, regulations are preferable to statutes since regulations "provide sufficient flexibility to permit experimentation and require less time for revision than do statutes."[164] A new agency, as opposed to one already in existence, is required since "none of the existing federal bureaus, agencies, or departments has enough background or is sufficiently in-

rate Relations, Southern New England Telephone Co.); M. HAMBURG, *supra* note 17, § 6.07[3], at 6-59 n.25; Quade, *supra* note 156, at 568.

162. E. LONG, THE INTRUDERS 183 (1966).

163. A. MILLER, *supra* note 9, at 227.

164. *Id.* at 229.

dependent . . . to be an effective guardian of individual privacy."[165] This agency need not be limited to cable privacy but can be expanded to regulate all privacy issues.

The federal privacy protection agency would also serve a second function. Similar to the Equal Employment Opportunity Commission,[166] this agency would be empowered to investigate a subscriber's complaint regarding an alleged privacy invasion.[167] If the agency believes there is enough evidence to show that an invasion of privacy occurred, it may then initiate a suit on behalf of those subscribers whose privacy has been violated.[168] If the agency does not believe that enough evidence exists, then the aggrieved individual would be free to initiate his own private suit. The agency would follow this procedure to screen out frivolous or fraudulent complaints.

One objection to a private tort action is that a subscriber may be reluctant to bring a suit since he may not want additional people to be privy to his personal matters.[169] An aggrieved individual would probably be less reluctant to seek relief if another entity brings a suit for him. One would probably be more willing to reveal such maters to a party helping him rather than to his adversary in an open courtroom. In addition, the litigation costs will not deter an aggrieved subscriber since he will not be paying the bill.[170] Further, lawsuits will not be deterred because of problems in assessing damages; if damages are too difficult to assess, statutory damages would be available.[171] Allowing the agency to handle privacy suits would thus eliminate most of the problems which exist if *only* private suits were allowed. This function of the agency need not be limited to cable privacy violations. It is beyond the scope of this Note, however, to discuss any further applications of the agency.

CONCLUSION

There are three ways in which cable television threatens individual privacy: through the compilation of data in an individually identifiable manner, the release of personal information to outside sources, and the use of cable as a surveillance device. The most effective way of protecting the privacy of cable subscribers is through the Cable Communications Policy Act of 1984 and the amendments to it as proposed by this

165. *Id.* at 232.
166. *See* 42 U.S.C. § 2000e-4 (1982).
167. *See id.* § 2000e-5(b).
168. *See id.* § 2000e-5(f)(1).
169. *See supra* text accompanying note 67.
170. *See supra* text accompanying note 68.
171. *Id.*

Note. In addition, a Federal Privacy Protection Agency is needed to keep abreast of the changes in this emerging technology, to propose regulations, and to enforce the provisions of the law.

Finally, it must be remembered that

> [a]n intrusion on our privacy threatens our liberty to do as we will, just as an assault, a battery or imprisonment of our person does. . . . Unlike many other torts, the harm caused is not one which may be repaired and the loss suffered is not one which may be made good by an award of damages. The injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered.[172]

Because the injury sustained from an invasion of privacy is abstract and difficult to measure, it is important to prevent the injury from occurring.

Glen R. Segal

172. Bloustein, *supra* note 10, at 1002-03.