ISSUES IN ELECTRONIC TRANSMISSIONS: UPDATE ON PRIVACY

ANNE KEATY*
AL B. WILLIAMS**

I. INTRODUCTION

The Internet has made private information more easily available to anyone and everyone. Geographical and political borders are easily transgressed, as are the physical walls of businesses and homes. Private information can be accessed with or without an individual's consent by surveillance or monitoring of businesses, employees, and private citizens; private information can be inaccurately transmitted or stored, distorting the truth about businesses and individuals; private information can be collected, combined, manipulated and disclosed for commercial and non-commercial reasons. Further, the Internet does not stop at national boundaries.

Many individuals are completely unaware of these invasions of their privacy, and some are not concerned. Many people are aware, but are willing to trade the benefit of having better access to information in return for "giving up" their own personal information. They may or may not be aware of the consequences that this trade off may have in the future. Those who are aware and concerned are looking for ways to protect against electronic invasions of privacy without stifling individual freedom and creativity and its accompanying monetary incentives on this new frontier.

This article will examine the traditional right to privacy in the context of electronic communications. The authors will explore the application of the right to privacy and provide an overview of industry responses and federal legislation relevant to the right to privacy in the world of electronic communications.

II. LIMITATIONS OF USING CONSTITUTIONAL AND STATUTORY LAW TO PROTECT INDIVIDUAL PRIVACY

In the United States, the idea of a legal right to privacy has its roots in common law tort actions.[1] The concept is found in the Bill of Rights of the United States Constitution in the First, Second, Fourth, Fifth and Fifteenth amendments, as recognized by the United States Supreme Court in cases such as *Griswold v. Connecticut*[2] in 1965 and *Roe v. Wade* in 1975. In *Roe* Justice Harry A. Blackmun stated:

> [T]he court or individual Justices have, indeed, found the roots of that right in the First Amendment, . . . in the Fourth and Fifth amendments, . .

* Anne Keaty, Associate Professor of Legal Studies, University of Louisiana at Lafayette
**Al B. Williams, Professor of Management, University of Louisiana at Lafayette
[1] RESTATEMENT (SECOND) OF TORTS § 652A (1977).
[2] 381 U.S. 479 (1965).

> . in the Ninth amendment, . . . or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment.[3]

The First Amendment prevents government intrusion into speech that is published or distributed electronically. Obscenity, however, is not protected in cyberspace anymore than it is in physical magazines, pictures, etc. Because encrypted data is classified as munitions, the Second Amendment may protect against the government's classification and regulation of encryption software as "munitions." The Fourth Amendment has been used by the Supreme Court to protect against government action of unreasonable searches and seizures in interception of telephone conversations and electronic eavesdropping on oral conversations[4] and to prevent government intrusion into a citizen's e-mail[5] and computer files[6] without a warrant. Video surveillance while at work was questioned in *Vega-Rodriquez v. Puerto Rico Telephone Co.,*[7] in which the court found that there was no reasonable expectation of privacy, declining to prescribe a test to be used and saying these cases must be decided on a case-by-case basis.[8] The Fifth Amendment protects against government-compelled self-incrimination and might be used to protect an individual against forced revelation of a password, even if the computer files could be searched pursuant to a valid warrant.[9]

There are multiple federal statutes that protect individual privacy,[10] but leave many important individual privacy issues totally unregulated. Since the electronic revolution, the federal government has been slow to regulate for many reasons. Political, social, and economic forces have resulted in the United States government holding back and letting industry have a chance to create its own solutions to the privacy problem. In addition to the reluctance of Congress to stifle invention and, perhaps, infringe on other Constitutional rights, the transition to electronic communication is progressing so fast that the lawmakers would have a hard time keeping up if they wanted to. It seems, in looking back over the last several years, that the reluctance has paid off somewhat in that private industry has created and continues to create its own solutions.[11] Because laws have not been drafted within any master framework, besides leaving some areas unregulated, these laws sometimes conflict with each other.[12]

Unlike the Bill of Rights and the implied privacy protections, some state constitutional provisions expressly protect personal privacy and apply to the private sector, as well as the governmental sector. Ten states have constitutional protection of privacy.[13] Some state constitutions (Pennsylvania and New Jersey) extend the right of

---

[3] Roe v. Wade, 410 U.S. 113, 152 (1973).
[4] Katz v. United States, 389 US 347 (1967).
[5] Minnesota v. Solson, 495 U.S. 91,95 (1990); United States v. Maxwell, 45 M.J.406, 417 (Armed Forces Ct. App. 1996).
[6] United States v. Kennedy, 81 F. Supp.2d 1103 (D. Kan. 2000).
[7] Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174 (1st Cir. 1997).
[8] *Id*. at 178.
[9] GERALD FERRERA, STEPHEN LICHENSTEIN, MARGO REDER, RAY AUGUST, & WILLIAM SCHIANO, CYBERLAW 191 (2001). *See also* United States v. Doe, 465 U.S. 605 (1984).
[10] See Appendix B.
[11] See Appendix A.
[12] For example, Cable TV companies who are also Internet providers have to keep customer choices of viewing private, but have to monitor as an Internet service provider.
[13] *See* EDWARD CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW (1996).

privacy to the records of telephone numbers dialed.[14] Some states (Florida, California, Colorado, and Pennsylvania) have constitutional protection for banking information.[15] Many states have enacted statutes similar in purpose and function to the federal privacy laws. Freedom of information and public records acts are prevalent in state law,[16] making computer data or information in government electronic data processing equipment subject to disclosure. States have passed laws similar to the Electronic Funds Transfer (EFT) Act, regulating the disclosure of EFT records, and laws similar to the federal wiretapping laws and electronic surveillance laws.[17] The National Conference of Commissioners on Uniform State Laws adopted a Uniform Information Practices Code (UIPC) in 1980 to provide a uniform law on privacy and access to information maintained by state and local governments. Article 2 of the UIPC deals with Freedom of Information and Article 3 deals with disclosure of Personnel Records.[18] While there is a growing accumulation of electronic environment cases under state law,[19] the laws are usually recently enacted and of a patchwork nature in every state.

The European Union (EU) enacted the EU Privacy Directive on October 4, 1998, which recognized data privacy as a fundamental human right, and forced its member states to adopt uniform laws to protect personal data collected by governments or for business purposes. The law does not address the issue of data collected for household or personal purposes. The EU Directive prohibits the transmission of personal data to countries like the United States that do not offer citizens privacy protection as set out in the EU Directive. After much negotiation, the U.S. Department of Commerce's Safe Harbors were approved by the European Union on July 27, 2000. These safe harbors are now being tested, but there is evidence that privacy policies that companies place on websites, both in the European Union and in the United States are not actually being

---

[14] Patricia H. Nunley, *Privacy Issues in the Workplace: Avoiding the `Penalty Box' and the Employee 'Power Play,'* SO. L.J. 24, 26 (1996).

[15] LAW OF THE INTERNET § 6.01 (Aspen 2000).

[16] 1Guide to Computer Law (CCH) ¶ 14,300 (2000).

[17] *Id.* Connecticut has a law forbidding electronic surveillance of employees in areas that employees use for health or comfort. Nevada's law gives the employee a right to confront the person who has made the surveillance and respond to any allegations. In Maryland, legislation was proposed which would make it a criminal offense for anyone to use e-mail to annoy, harass or embarrass anyone and Virginia has proposed a statute that would prohibit e-mail messages containing profane, indecent or threatening language. Some state laws forbidding anonymous e-mails on the Internet have been banned as a violation of freedom of speech.

[18] *Id.* ¶14,350.

[19] *See, e.g.*, Flannagan v. Epson America, Docket No. 1990 No. BC 007036 (Sup. Ct. Los Angeles Co.) (finding that the e-mail in the workplace was not protected by the California statute protecting private e-mail from unauthorized interception); Bourke v. Nissan Motor Corp., No. BO68705 (Cal. Ct. App. July 26, 1993) (finding that the state statute did not protect the e-mail of an employee using a business-owned computer where the employee had signed a waiver agreeing that the computers were to be used for business purposes only); State of Washington v. Heckel, 95 Wash. App. 1056 (1999) (suit was filed by State Attorney General for alleged violation of Washington's new anti-spam law; McLaren, v. Microsoft Corp., 97-00095-f (116th Judicial District, Dallas County, TX) (finding employee privacy was not violated when employer accessed e-mail in employee's personal folder, even though employee had been given a password because the messages were not personal property of employee and somewhere in the transmission over the network and on the server the messages were accessible to third parties).

followed.[20] Individual countries outside the European Union have widely varying laws and responses to the privacy issues related to electronic communications.[21]

III. THE TORT INVASION OF PRIVACY AS A VIABLE OPTION

The tort of invasion of privacy is a traditional, well-recognized law that has been developed and interpreted in numerous cases. By 1960, the tort of invasion of privacy was recognized in approximately 30 states.[22] William Prosser's instrumental 1960 law review article identified four distinct causes of action for invasion of privacy: (1) unreasonable intrusion or intentional interference with a plaintiff's interest in solitude or seclusion (either in his person or in his private affairs); (2) public disclosure of private facts; (3) publicity which places the plaintiff in a false light; and (4) appropriation of the defendant's name or likeness for commercial benefit.[23] Over the years, the tort has played an important part in the protection of individual privacy in the non-electronic environment. Today, technology makes the accessibility to, duplication of, and combination of private information much easier, faster, and cheaper. It is proposed that the tort of invasion of privacy is now being used and can continue to be used successfully in cases involving privacy on the Internet, at least while federal, state, and international communities struggle to create statutory answers to privacy problems. In order to illustrate the present use of this tort, this article will classify the electronic environment cases brought on the grounds of the tort of invasion of privacy and analyze the cases according to the elements under each of Prosser's four theories.[24]

Next, some of the more common invasions of privacy in the electronic environment will be classified according to Prosser's four theories in an effort to encourage the use of the tort in the future as a cause of action in Internet privacy cases. In the electronic

---

[20] A consumer' s international survey reported that few United States and European sites abide by international privacy standards. The survey canvassed 751 sites and found that two-thirds of the sites collected personal data. Despite the presence of the EU Data Privacy Directive, the survey found that EU sites were no better than sites based in the United States. Internet Law News (BNA)(citing the survey at http://www.consumerinternational.org/news/pressreleases/fprivreport.pdf. (visited Jan. 25, 20010).

[21] *See* Data Directive (DPD), Council Directive 95/46/EC, 1995 O.J. (L 2281) 31.

[22] RESTATEMENT OF TORTS (SECOND) § 6552C (1977).

[23] William L. Prosser, *Privacy*, 48 CAL.L.REV . 383 (1960).

[24]There might seem, at first glance, to be an application problem in applying this traditional law to the electronic environment. Because of the instantaneous, easy, and inexpensive nature of electronic transmissions, the intrusion of accessing, viewing, and appropriating seem to happen all at once. However, this overlapping problem was already dealt with by courts' interpretation of the ECPA when a difference was recognized between the interception of telephone communications which may or may not have been simultaneously stored on a tape recording or paper, and the interception of electronic communications with its necessary *instantaneous* storage on at least one computer, as well as its potential for instantaneous disclosure. In *Jackson Games v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the court found that the Electronic Communications Privacy Act (EPCA) did not apply to storage on a computer because unlike the original Wiretap Act, the ECPA did not specifically speak to the issue of stored communication. In 1999, in *Konop v. Hawaiian Airlines, Inc.,* 2001 WL 13232 (9th Cir. 2001), the court found that there should be no distinction made between the protection given to electronic communications in transmission and that given to stored electronic communication because it is not possible to send an electronic communication without storing it.

environment, intrusions, appropriations, and disclosures are taking place, faster and more often than in the past. Therefore, the common law remedy for invasion of privacy should still have a rightful place in the electronic environment.

A. PROSSER'S FIRST THEORY OF INVASION OF PRIVACY: INTRUSION UPON SECLUSION

Traditionally, intrusion upon seclusion requires unreasonable intrusion into an area that is not public and the area in one in which an individual has a reasonable expectation of privacy.[25] The tort does not require disclosure and has traditionally been used to protect against eavesdropping.

What is intrusion in the electronic environment? Traditionally, intrusions were physical acts. Although physical wiretaps or "bugs" were considered intrusions,[26] there was a question as to whether electronic transmissions themselves were intrusions, since they were not always physical intrusions. One avenue used to answer this problem is to ascertain how the electronic transmission would be looked upon in other laws. In 1996 in *Sega Enterprises Ltd v. Maphia*[27] the court found that to borrow another's password, in the situation where permission was given by the legitimate owner of the password, in order to access to the bulletin board was not unauthorized access and there was no violation of the Stored Wire and Electronic Communications and Transactional Records Act.[28]

The following cases have recently found electronic transmissions to be trespass. Trespass was found in *Compuserve v. Cyper Promotions* when Cyber Promotions spammed Compuserve's customers[29] and in *America Online Inc. v. LCGM*[30] trespass to chattel was found and an injunction granted against spammers. Trespass was found again in *America Online, Inc. v. National Health Care Discount , Inc*.[31] In 1998 in *Micheals v. Internet Entertainment Group, Inc.,*[32] a district court in California found that there was an "intrusion" when a videotape depicting a couple engaged in sex was displayed on the Internet, holding that the intrusion did not have to be physical. In 1999 in *Creative Telecommunications, Inc. v. Breeden*[33] the plaintiff claimed invasion of privacy based on the defendant's interference with plaintiff's e-mail account while he was an employee. The claim was found to be subject to arbitration. In 2000 in *Realnetworks, Inc., Privacy Litigation*[34] plaintiffs alleged trespass to property and privacy claiming that RealNetworks' software products secretly allowed RealNetworks to access and intercept users' electronic communications and to store information without their knowledge or consent. This action also was found to be subject to arbitration. In 2000 in *United States*

---

[25] Restatement (Second) of Torts s 652B (1976 Main vol.)
[26] HENRY PERRETT, LAW AND THE INFORMATION SUPERHIGHWAY, 121 (2nd ed. 2000).
[27] 948 F. Supp. 923, 930 (N.D. Cal. 1996).
[28] 18 U.S.C. §§ 2701, 2702 (West 2001).
[29] 962 F. Supp 1015 (S.D. Ohio 1997).
[30] America OnLine, Inc. v. LCGM, 46 F. Supp.2d 444, 445 (E.D. Va. 1998).
[31] 121 F. Supp.2d 1255 (N.D. Iowa 2000).
[32] 5 F. Supp.2d 823 (C.D. Cal. 1998).
[33] 120 F. Supp 2d 1225 (D. Hawaii 1999).
[34] 2000 WL 631341 (N.D .Ill. 2000).

v. Kennedy,[35] the defendant was indicted for the intentional receipt of child pornography, and filed a motion to suppress evidence obtained from his computer files. The court noted that Kennedy had not claimed intrusion. The court denied Kennedy's motion because, among other things, there was no Fourth Amendment protection for his computer files when searched by an anonymous caller and the Internet service provider. In 2001, in *Supnik v. Amazon.com, Inc.* [36] the plaintiffs asked the court for class certification to bring a class action against Alexa Internet, which created, and Amazon, which distributed, a software program which enabled Alexa and Amazon to intercept and access users' personal information in violation of their rights to privacy. The court certified the class and a decision is pending.

The second element in the theory is that the area of concern has not already been made public. In *Smyth v. Pillsbury Co.*,[37] the employee had no reasonable expectation of privacy in e-mails he voluntarily sent to his supervisor, notwithstanding assurances to the contrary. Because when he sent e-mail over the company server the court said that the information was made public. The defendant in *Michaels* contended that because the couple had already released part of the sex videotape in Holland, that the tape was already public. The court disagreed because only part of the tape was publicized on a Dutch Internet site and the rest of the tape was not "matters of public knowledge."[38] In 1999 in *United States v. Hambrick*,[39] the court found that when Hambrick gave his real name to the service provider in the process of setting up his screen name, he had already made the connection between his real name and his screen name public knowledge. He knew, the court said, that the employees of the service provider would see his real name and there was nothing in his agreement with them that would keep them from telling anyone except the government because of the Electronic Communications Privacy Act. In 1999 in *Akella v. Michigan Department of State Police*,[40] the court found that a convicted sex offender had no reasonable expectation of privacy in the listing of his addresses on the sex offender registry on the Internet because the information was already a matter of public record (albeit less convenient to access).

If the area is not already public, the third element of this theory is that it must be an area that, when entered upon, would cause the reasonable person to feel embarrassment or humiliation. The intrusion into one's private affairs must be highly offensive to the reasonable person.[41] In 1967, in *Katz v. United States*,[42] the court found that the government intruded into an area where the plaintiff would expect privacy by wiretapping a public telephone booth that the plaintiff was known to use. The plaintiff had, the court said, a reasonable expectation of privacy even in a public phone booth. In 1998 the defendant in *Michaels*[43] claimed that, because the female was an actress whose acting career was based on sex, she had no reasonable expectation of privacy into this area of her life and that the acts on the tape were not private. The court found that the sex

---

[35] 81 F. Supp.2d 1103 (D. Kan. 2000).
[36] 2000 WL 1603820 (W.D. Wash. 2000).
[37] 914 F. Supp. 97 (E.D.Pa. 1996).
[38] *See supra* note 31 and accompanying text.
[39] 55 F. Supp 2d 504 (W.D. Va. 1999).
[40] 67 F. Supp.2d 716 (E.D. Mich.).
[41] RESTATEMENT (SECOND) OF TORTS § 652B.
[42] 389 U.S. 347 (1967).
[43] *See supra* note 32 and accompanying text.

acts on the tape were, nevertheless, private. In 2000, in *Panayi v. Northern Indiana Public Service*[44] the court did not reach the issue of the plaintiff's right to an expectation of privacy in his Internet access files because the right of his employer to see his files was preempted by the collective bargaining agreement.

In two Fourth Amendment cases, the court found a reasonable expectation of privacy. In 1998 in *United States v. Barth*[45] the court held that by placing files in a computer storage device such as a hard drive, the owner manifested a reasonable expectation of privacy in contents of those files. In 1999, in *United States v. Gray*[46] the court found that the computer files of a defendant who was charged with accessing a government computer and possession of child pornography, were entitled to the same protection as written files under the Fourth Amendment but, like paper files, innocuous-looking computer files could be examined to determine whether they fall into a category of those files covered by the warrant.

Usually names and addresses are not considered private areas of concern since people do not think of these as private areas because revelation of them would not cause embarrassment or humiliation. In 2000 in *Jessup-Morgan v. America Online, Inc.*[47] plaintiff as a subscriber to AOL had posted an Internet message on AOL meant to embarrass and harass her boyfriend's ex- wife. The lawyer for the ex-wife subpoenaed the real name of the plaintiff from AOL and AOL provided it by looking at records and matching the screen name to the real name. Plaintiff then sued AOL for invasion of privacy in revealing her name. The court did not reach issue of whether the disclosure violated a right to privacy and held that Virginia had no invasion of privacy tort for intrusion upon seclusion or disclosure of private facts.

B. PROSSER'S SECOND THEORY OF INVASION OF PRIVACY: PUBLIC DISCLOSURE OF PRIVATE FACTS

The second theory requires disclosure to the public of information that the reasonable person would not want made public. What is meant by "public disclosure"? What is meant by "private facts?" And are these facts different from the "private areas" in the tort of intrusion into seclusion?

The first element seems to be the same: the facts cannot already be public. For example in 1975 in *McNutt v. New Mexico State Tribune Co.*[48] the court found that revealing police officers' names and addresses did not constitute a public disclosure of personal matters because an officer's home address is a public fact that is already public.

The second element of "private facts" carries the requirement that the plaintiff will be embarrassed or damaged by the facts themselves or that the revelation of the facts themselves may have a "chilling affect" on the plaintiff's personal choices by letting the public know his or her personal choices. In 1975 in *Cox Broadcasting Co. v. Cohn*,[49] the

---

[44] 109 F. Supp.2d 1012 (N.D. Ind. 2000).
[45] 26 F. Supp.2d 929 (W.D. Tex.).
[46] 78 F. Supp.2d 524 (E.D. Va. 1999).
[47] 20 F. Supp.2d 1105 (E.D. Mich. 1998).
[48] 538 P.2d 804 (N.M. Ct. App. 1975), *cert. denied*, 540 P.2d 248 (N.M. S.Ct. 1975).
[49] 420 U.S.169 (1975).

defendant had revealed the name of a deceased rape victim. The court found the victim's name was already a matter of public record. In 1995, in *Religious Technology Center v. Netcom On-Line Communication Services*,[50] the plaintiff sued to enjoin the publisher from disclosing church documents on the Internet. The court found that since the records were already available on the Internet they could not be a "trade secret." In 1998, the *Michaels* court found that there was disclosure of private facts with the playing of a videotape plaintiffs had made depicting themselves engaging in sexual intercourse. Even though the plaintiffs had previously shown the tape on a Holland website, the court found the tape was not "public knowledge."[51] In 1999, in *Akella v. Michigan Department of State Police*[52] the plaintiffs brought suit challenging the constitutionality of the act requiring registration of sex offenders. The court found the plaintiffs had no privacy interest in preventing compilation and dissemination of truthful information that was already a matter of public record. In *United States v. Kennedy*,[53] the defendant was indicted for the intentional receipt of child pornography, and filed a motion to suppress evidence obtained in violation of his Fourth Amendment rights when his service provider divulged his subscriber information. The court found that the plaintiff had made his subscriber information public when he entered into the agreement with his provider.

C. PROSSER'S THIRD THEORY OF INVASION OF PRIVACY: PUBLICLY DISCLOSING INFORMATION ABOUT A PERSON THAT CASTS HIM OR HER IN A FALSE LIGHT.

The information disclosed under the third theory does not have to be private, but does have to intentionally create a false impression and make the public think something about a person that would be reasonably offensive to the person depicted.[54] If the person depicted is famous or has put himself or herself in the public eye, then the false portrayal must have been done with malice.

In 1998, in *Seidl v. Greentree Mortgage Co.*,[55] the plaintiff sued for false light invasion of privacy claiming that the defendant used the plaintiff's domain name e-mail identifier in its bulk electronic mail advertising campaign. The court held that the company did not have the standing to bring a false light claim because it was not an individual (the domain name belonged to corporation that the plaintiff had incorporated). In 2000, however, an Indiana court of appeals in *Feisher v. University of Evansville*[56] found that a corporation (a university) could maintain an action for invasion of privacy. In 1997 in *Seale v. Gramercy Pictures*[57] the plaintiff, an activist, sued the producers of a motion picture for use of his likeness by making an actor in a movie look like him and in using photos of the actor who looked like him on the brochure enclosed with a compact disc sound track to the movie. The activist lost because he was a public figure and did

[50] 923 F. Supp. 1231 (N.D. Cal. 1995)
[51] 5 F. Supp.2d 823, 840 (C.D. Cal. 1998).
[52] 67 F. Supp. 2d 716 (E.D. Mich. 1999).
[53] 81 F. Supp. 2d 1103 (D. Kan. 2000).
[54] RESTATEMENT (SECOND) OF TORTS § 652D (2000).
[55] 30 F. Supp. 2d 1292 (D. Col. 1998).
[56] 727 N.E.2d 783 (Indiana Ct. App. 2000).
[57] 964 F. Supp. 918 (E.D. Pa. 1997).

not prove that the likeness portrayed a false image with actual malice. In 2000, in *Zeran v. Diamond Broadcasting*[58] the plaintiff sued a radio station after the announcer read the plaintiff's telephone number from a hoax website that depicted the plaintiff as being an advocate of the Oklahoma bombing. (The hoax website developer could not be identified.) The court found that the plaintiff did not show that the talk show hosts exhibited the standard of recklessness (intent) required to recover for false light invasion of privacy.

D. PROSSER'S FOURTH THEORY OF INVASION OF PRIVACY: A PPROPRIATION OF ONE'S NAME OR LIKENESS FOR BENEFIT

In *Feisher v. University of Evansville*[59] an Indiana Court of Appeals found that a corporation (in this case a university) could maintain an action for invasion of privacy for appropriation of its name for derogatory purposes on defendant's own website. The court found that a corporation was an individual and that, although a corporation could not have "hurt feelings," it could protect its interest in its name.

In *KNB Enterprises v. Matthews*[60] the owner of a copyright to erotic photographs of models which had been displayed without authorization for profit on the Internet website brought suit against the website operator. The Court of Appeals of California found that the tort action for misappropriation of name, photograph, or likeness was not preempted by federal copyright law because it was not equivalent to a copyright infringement claim.

One exception to liability under Prosser's Fourth Theory is the First Amendment right of "newsworthiness."[61] In *Stern v. Delphi Internet Services Corp.*,[62] Howard Stern sued a company that provided access to a computerized database service, for commercial misappropriation of his name and picture to advertise its electronic bulletin board for debate on Stern's candidacy for office of governor. The court held that the company was a news provider, such as a bookstore, and that the use of Stern's partially nude photo fell within the "incidental use" exception to the misappropriation tort. Sterns candidacy was a matter of public interest related to the advertisement. As discussed previously, in *Michaels* the court found that the newsworthiness exception to the right of privacy was outweighed by the right of the couple to conduct their sexual activities in private.[63]

The authors propose that the gathering and compiling of facts about an individual into a database may be considered a "likeness" that when sold or used for commercial purposes would be actionable under this theory as well as under the theory of public disclosure of private facts.

---

[58] 203 F.3d 714 (10th Cir. 2000).
[59] 727 N.E.2d 783 (Ind. Ct. App. 2000).
[60] 92 Cal. Rptr.2d 713 (Cal. Ct. App. 2000).
[61] RESTATEMENT (SECOND) OF TORTS § 652C (1976 Main Vol.)
[62] 626 N.Y.S.2d 694 (S.Ct. N.Y. 1995).
[63] *See supra* note 30 and accompanying text.

IV. PRIVACY ISSUES CLASSIFIED ACCORDING TO PROSSER'S INVASION OF PRIVACY THEORIES

Potential invasions of privacy in the electronic environment can be organized according to Prosser's common law causes of action.[64]

A. INTRUSION

1. AUTHORIZED ACCESSING AND VIEWING

Intelligent Agents encourage authorization of access to personal information. Authorized accessing is not an invasion of privacy. Many people willingly disclose private information. For example, Firefly Network is a company which asks users to give personal information about themselves, to profile themselves, and then Firefly, with the use of "intelligent agents" software created by Massachusetts Institute of Technology, identifies and recommends web sites for the user based on the user's tastes. Data containing the user profiles are stored and constantly expanded by comparing the profile anonymously to other similar anonymous profiles. Firefly's main areas of concentration have been music and motion pictures, but they are expanding coverage to other areas of interest.

Reuters New Media is using Firefly to help its users find news stories of interest to them. Recom Mentor is working on software that will be able to predict a user's choices in one area of interest based on the user's preferences in another area of interest. For example, golfers presumably would like to see advertisements for golf products. BroadVision also uses intelligent agents in their software. CyberGold uses intelligent agents to target advertising based on a user's preferences. NetRadio Network uses personal information supplied by the user and presents "play lists" individualized for each user, including advertising customized to the user's tastes. While the authorized access itself is not an invasion of privacy, what is done with the gathered information may be unauthorized viewing, appropriation, or disclosure.

2. UNAUTHORIZED ACCESSING AND VIEWING

Software systems that allow the merging of e-mail and voice mail and fax systems enable all three modes of communication to be received into one mailbox and accessed by computer or telephone. This integrated messaging system complicates the security and privacy of the messages and allows easier unauthorized access.

The storage of e-mail messages on World Wide Web sites, rather than private systems, increases the risk of invasion of privacy because the mere volume of messages raises a question as to whether these messages can be adequately protected by the particular web site. Use of firewalls to separate these messages from unauthorized access is not as easily done on a web site as it can be done on a private Intranet system. Some servers used are outdated and easily accessed by new software.

---

[64] *See generally* Law of Electronic Commerce, *supra* note 15, and SCOTT ON COMPUTER LAW (Aspen 2000), for information on the different kinds of invasions of privacy on the internet and the industry attempts to protect against invasions.

Search engines can now search chat rooms, newsgroups, and bulletin boards instead of just web sites. Once into those rooms, e-mail addresses and the e-mail messages themselves can be viewed by the search engine. DejaNews enables the searcher to search newsgroups using a person's name and to find out a great deal of information about the person's tastes and identifying information, creating a profile of that individual. Profile information may reveal information that is illegal to obtain from the individual in any other way, such as an interest in a particular disability or disease. Search engines can now operate on both the Internet and a company's Intranet and Extranet. Search engines used for Internet searches are also being used very effectively for internal data searches within businesses. Two or more businesses' Intranets are some times connected together by an Extranet. Search engines that do both internal and external searches open the door to monitoring by the employer of the employee's use of the Internet, including e-mail messages and sites visited. On the other hand, employers have suffered great economic loss from breach of security and theft of company data, as well as loss of time while employees surf the web. The NASA web site, for instance, was vandalized, and Microsoft itself has been subject to hacker attacks.

Hive computers and spiders are enabling search engines to become more sophisticated and capable of searching more thoroughly. Inktomi is an example of a search engine that uses a network of workstations to provide computing power (this process is called hive computing), and has built on the keywords already used by Lycos and Alta Vista to create a more comprehensive key word index. The use of "spiders" to crawl through the web from site to site through the links between Web locations has enabled the creation of enormous indices of words and web sites. New search engines search with concepts instead of words. Architext Software from Excite allows sites to be hit that contain different words, but cover similar subjects.

Intelligent agents can be used destructively. Intelligent agents can overload web site servers with requests, or can prevent or block the delivery of Internet messages. Viruses such as the "Russian New Year" and the Melissa virus and its mutant offspring are intelligent agents that are programmed to go into the visitor's computer and cause damage. Streams of search words can be watched for entertainment. A steady stream of search words entered on Excite's Magellan search engine is available for viewing by the public. While these words do not reveal the identity of the individual searching, the individual does not know his or her search words are being watched.

Unauthorized access to legal and medical records is an extensive problem entailing both professional ethics and the law. Most professional codes have not caught up with electronic transmission activity to the extent that these professionals are many times unknowledgeable and usually uncertain of the consequences of talking to their clients or sending information electronically. The clients themselves may demand electronic communication.

B. APPROPRIATION

1. UNAUTHORIZED ACCESSING AND VIEWING AND APPROPRIATING

Cookies are the text files created by the web site proprietor with or without the consent of the visitor when a person visits the web site. The web site proprietor's server

appropriates the e-mail address of the visitor, the URL of the site from which the visitor last came, the type of search engine used and the type of computer used. The website's server generates a file for the visitor and stores the visitor's information in this text file. This text file is in turn stored on the visitor's hard drive, and can be accessed by the web site on the visitor's next visit. While this information does not include a personal identification of the visitor, when web sites ask visitors to register by giving personally identifying information so that the web site can better serve the visitor, this personal information can be matched with the cookie, and the web site proprietor now has personally identified the visitor with his or her e-mail address.

Webthreads may be used even if cookies are not. Some web sites do not use servers that can generate cookies, and some visitors do not register or use on-line service providers who do allow cookies to be stored on the visitor's hard drive. However, a website's server may use Webthreads software to keep track of a visitor's use of this particular web site. Information that can be appropriated is the browser used by the visitor, the pages visited, the time spent on each page, and the choices made by the visitor as he or she moves through the web site. The web site can use this information immediately to customize the current web site to the visitor's tastes.[65] Andromedia's Aria World Wide Web Recording and Reporting System is another product similar to Webthreads, but the creators have refused to allow their product to identify and match personal information with the information about the sites visited.

IBM's Internet Marketing Server Software (IMS) provides similar marketing information to web site businesses.[66] DoubleClick is software used by web site operators and advertisers which tracks the sites browsed on a particular web site. Based on this information, the software profiles the visitor and then directs that certain types of advertising be presented to this visitor based on his or her browsing pattern. Similar analytical software is WebTrak. Abacus Direct gathers data on consumer purchasing patterns in catalogs. Kid.com is a web site, which provides prizes for children to give personal information. This particular problem of gaining information from children is one of the few particular problems that have been regulated by law.

Clickstreams are another source of information about the visitors to a web site. A visitor leaves an electronic marker at each web site visited and the trail of these markers is called a clickstream. Information about the visitor can be gathered from the clickstream by the web sites visited.

2. UNAUTHORIZED ACCESSING, VIEWING, APPROPRIATING AND DISCLOSING

A web site proprietor may purposefully sell or trade the information gathered about visitors as a valuable commodity for marketing purposes. Even if not disclosed for profit, private electronic data, such as e-mail and web sites visited can simply be an invasion of solitude or "made public" to the embarrassment of the parties involved Electronic data, including e-mail, can be considered records, and therefore can be susceptible to access

---

[65] LAW OF THE INTERNET, *supra* note 15, at § 6.03 (*citing* Doug Henschen, *Software Lets Web Sites Track and Interact with Visitors*, DM NEWS, Aug. 19, 1996, at 19).
[66] *Id.*

under state and federal laws such as the laws of evidence and the federal Freedom of Information Act.[67]

P-TRAK is software developed by Lexis-Nexis. Subscribers to P-TRAK can purchase certain personal information about a person, which P-TRAK gathers legitimately from credit records. Whereas P-TRAK voluntarily abstains from giving out social security numbers, a social security number input into P-TRAK will reveal the number's owner. Anyone may access his or her own personal P-TRAK information at a fee below the standard subscriber fee. This information is a valuable commodity to anyone trying to get information on another person, and is also valuable to marketing and sales people.

E-mail list providers are companies that are gathering and making lists of e-mail addresses, many times with the additional information provided willingly by people when they register on-line for different services, and selling these lists to marketers. The result is that e-mail addresses become very vulnerable to abuse. The ability to forward private e-mail to a worldwide audience is much easier and cheaper than forwarding private information on paper or telephone or fax, and therefore more likely to be done, making it a potential privacy problem. A website has the ability to serve as a video distribution center such as the situation in which a video recording of the front door of a brothel in Norway was connected to the Internet, showing everyone who entered or left the establishment. Websites can be used as distribution centers by the government of Criminal Records such as the case in which Florida made information about sexual predators available on-line.

V. CONCLUSION

In cases involving privacy and the Internet, the courts are using common law tort theories of invasion of privacy. While these tort theories have the drawback of being less certain in their application than federal statutes, they offer the advantages of allowing the plaintiff to ask for mental suffering and punitive damages if intent can be proved. In addition, tort actions may cover situations that lie outside the present Constitutional and statutory protections.[68]

The use of software to gather, compile and then sell or otherwise make commercial use of names, addresses, and personal choices, particularly when these personal choices are identified with an individual, would be prime areas for use of the tort theories of invasion of privacy by intrusion, publicizing private facts and misappropriation of one's name or likeness for commercial benefit. If the purpose of the intrusion tort is to prevent unreasonable embarrassment and if the purpose of the "publicity tort" is to prevent the "chilling effect" public knowledge has on an individual's decision to pursue a particular interest, and if the purpose of the misappropriation tort is to prevent the use of person's name or likeness for the commercial benefit of another, then the compilation of databases should be actionable under these theories.

---

[67] 5 U.S.C.A. § 552 (West 2000).
[68] *See* Perrett, *supra* note 26.

Appendix A

I. INDUSTRY SOLUTIONS[69]

A. INDUSTRY SOLUTIONS TO UNAUTHORIZED ACCESS: BLOCKING AND MONITORING SOFTWARE

Encryption Software, seemingly the answer to many of the problems noticed above has become the age-old "double edged sword." The Pretty Good Privacy (PGP) electronic privacy program, created by Phil Zimmermann is virtually impervious, even to the United States government. The U.S. government always wants to be able to break the encryption code for national security purposes. Thus, the government has prohibited the export of PGP outside the United States.[70] This law has been challenged successfully as a violation of the First Amendment in *Berstein v. United States Dept. of Justice*.[71] A different result obtained in *Junger v. Daley.* [72]

Nevertheless, the problems encountered by businesses maintaining Internet connectivity have been addressed by multiple governmental and private studies. These studies indicate that staggering losses are being borne by United States organizations as a result of privately motivated "surfing" by employees while at work and computer-related security breaches. At this time, the security of private businesses are only as good as the policies set by that business.[73] Lack of government regulation and the encryption problem have spurred industry on to create alternate ways to protect themselves. The following are some of the inventions founded through necessity and competition by industry.

Security Breach Prevention Hardware and Software is used to protect against unauthorized access. Oracle and Identix have created new biometric authentication systems that rely on biological indicators as the keys to the system instead of passwords. IBM has created chips and transmitters built into employee identification badges to relay clearance data that is read by scanners. "Asset ID" uses the identifying information of each computer as a password.

"Reject Cookie" Software, such as PrivNet and Internet Fast Forward has been developed which reject cookies, not allowing them on the visitor's computer. Screening Software installed on the user's computer blocks outgoing information of choice, such as credit card information, addresses, and the like. Cybersitter, Net Nanny, and Cyber Patrol all offer these filtering capabilities "Reverse Cookie Software" can be used to monitor web sites visited to find out which ones deposit cookies on the visitor's computer. Software has been developed which, when installed on the user's computer, reports all web sites visited by a user of a particular computer or system. This software can be used by a parent to monitor children or an employer to monitor the web pages visited by the

---

[69] *See generally* LAW OF ELECTRONIC COMMERCE (Aspen 2000), LAW OF THE INTERNET (Aspen 2000), and SCOTT ON COMPUTER LAW (Aspen 2000) for information on the different kinds of invasions of privacy on the internet and the industry attempts to protect against invasions.

[70] CLARKSON, MILLER, JENTZ, CROSS, WEST'S BUSINESS LAW 170 (7th ed. 1998).

[71] 176 F.3d 1132 (9th Cir. 1999).

[72] 8 F.Supp.2d 708 (N.D .Ohio 1998).

[73] Guide to Computer Law, *supra* note 16, at ¶ 15,230.

employees while at work, and also to know which web sites might have deposited cookies on the user's computer.

B. INDUSTRY SOLUTIONS TO UNAUTHORIZED ACCESS, VIEWING, APPROPRIATION, AND DISCLOSURE

Certification of the Security of the Web site is one of the recent industry developments in security. Competition in the market place has led businesses to explore different methods of beating the competition by having a more secure web site than the competitors. The National Computer Security Association (NCSA) has been organized by computer security experts who will "certify" individual web sites so that users may determine the extent of each web site's security. This certification is accomplished by evaluation of essential criteria, such as security policies and procedures of the site, and the vulnerability of the site to hackers, whether the web site uses cookies and the strength of its firewalls.[74]

eTRUST is an organization trying to promote on-line privacy of personal data by its "trustmark" system. The system rates the level of security of a member web site and assigns it one of three categories of certification: anonymous or no-exchange (no personal data is collected from the user), one–to-one exchange (data collected will only be used by this one web site), and third party exchange (data collected but only provided to specified third parties with the user's consent). Adherence to the requirements of the category is constantly monitored by eTRUST and by independent auditors.

Another privacy-rating solution is the Platform for Internet Content Selection (PICS). Under this system web sites can be audited, rated and labeled according to the degree of privacy and security afforded visitors. The users' browser software can read these labels and access only those sites that provide adequate privacy and security. Users can access insecure sites or sites which do not protect privacy according to their own personal decisions and incentives offered by the web site owners and proprietors. The underlying problem with this solution is that certain visitors, such as children, may not be able to make an informed choice as to how much privacy they want. Employees may not care.

New businesses are developing and offering "certified e-mail." Deloitte & Touche and a bank, Thurston Group, have jointed to create NetDox that will make e-mail more secure and will also certify the receipt of messages. An electronic thumbprint is used to track each document and to make certain its delivery. Plans include joining forces with United Parcel Service. The U.S. Postal Service is developing similar capabilities.[75]

Use of an intermediary who assigns anonymous codes is another security solution. With this method, an intermediary gives the user a code, and the websites that the visitor visits have access only to this code and anonymous demographic information, rather than the personally identifying information of the user. The user tells the intermediary when the personal information should be sent to the website, and then the information is sent only to websites that have contracted with the intermediary to maintain certain security on their websites. An example of this solution is Internet Profiles (I/PRO) and its

---

[74] LAW OF THE INTERNET, *supra* note 15, at § 6.03.
[75] *Id.* at § 6.02.

registration system, I/CODE. Firefly Network provides a code name to protect the personal identity of subscribers.

Software has been created which only allows access to authorized information selected by the user. Some of the major internet companies such as Microsoft and Netscape have teamed up to support the adoption of the open profiling standard (OPS) where users select the type and amount of personal data that they will allow to be shared. This data is stored on the user's computer with particular software that only releases the data with authorization from the user. The system destroys the use of cookies and other ways in which web sites try to acquire user data. The system had been submitted to the World Wide Web Consortium for adoption.

Remailers are mechanisms created to permit e-mail messages to be sent anonymously and still enable the sender to be able to receive responses to the original message. This is accomplished by sending the e-mail through a remailer who wipes out the sender's e-mail address and sends the message out under the remailer's return address. At the same time, the remailer assigns a code to the sender that is kept on file, so when the message is answered, the answer can be sent by the remailer to the coded sender. One concern is that people might act irresponsibly or even illegally if they can act anonymously. C2Net provides privacy capability for Internet users in a number of ways including offering anonymous Internet accounts, using remailers and using pseudonymous servers as well as access to software.

Industry association guidelines are being created and promulgated to members describing ways in which members can be responsible in protecting consumer privacy. Associations such as the Direct Marketing Association (DMA) and the Internet Advertising Association (IAA) are involved, but more associations are predicted to join this self-regulation movement.

Major International Businesses' Joint Guidelines have been developed by big businesses engaged in e-commerce, such as IBM, AOL, Time Warner, Fujitsu, Toshiba, France Telecom, and Bertelsmann to regulate the use of personally identifiable information on-line. Examples are the Center for Democracy and Technology's Report on on-line privacy,[76] and the guidelines developed by Smart-Card.[77]

Non-profit organizations are becoming active in the education of users. The Privacy Rights Clearing House is a nonprofit organization that is engaged in efforts to educate the public about on-line privacy issues. Another organization engaged in similar efforts is the National Consumer League though its involvement in the Online Public Education Network (Project OPEN).

Industry password sharing restrictions are being used to prevent password sharing. Software will identify the user by zip code, or will prevent access by the same password more than a certain number of times during the day. Economic incentives have proven to be effective in discouraging password sharing. Systems such as ESPN are using additional information that might make subscribers less likely to share passwords. The Wall Street Journal requires the individual who shares his or her password to pay for purchases of anyone to whom the subscriber gave the password.

---

[76]The Center for Democracy and Technology's Report on On-line Privacy, *Communications Privacy in the Digital Age*, available at http://www.cdt.org/digi_tele/9706rpt.html.

[77] *Smart Card Industry Recommends Steps to Protect Consumer Privacy*, Dow Jones Front Page, America Online (May 8, 1997).

New Organizations are being formed to study and to respond to security breaches. The Computer Emergency Response Team (CERT) of Carnegie Mellon University is a joint government and industry effort to respond to and to resolve internal network security breaches. Private security consultants are becoming popular. The Manhattan Cyber Project conducts studies of threats to Internet security.

Trade associations such as "Online Privacy Alliance" are working with member organizations to promote the development and implementation of sound privacy policies.[78]

[78] LAW OF ELECTRONIC COMMERCE, *supra* note 64, at §14.06 (*citing* http://www.privacyalliance.com).

Appendix B

FEDERAL LAW PRIVACY PROTECTIONS

1. 1968 The Federal Wiretap Act[79]
2. 1970 The Fair Credit Reporting Act[80]
3. 1974 Family Educational Rights and Privacy Act[81] (FERPA)
4. The Privacy Act of 1974[82]
5. The Right to Financial Privacy Act of 1978[83]
6. The Electronic Funds Transfer Act[84]
7. The Small Business Computer Security and Education Act[85]
8. The Cable Communications Privacy Act of 1984[86]
9. 1986 The Electronic Communications Privacy Act[87]
10. The Security Act of 1987[88]
11. The Video Privacy Protection Act of 1988[89]
12. 1988 Computer Matching and Privacy Protection Act[90]
13. 1991 The Telephone Consumer Protection Act[91]
14. 1993 Clipper Chip Announcement[92]
15. 1994 The Computer Fraud and Abuse Act[93]
16. 1996 Telecommunications Act of 1996[94]
17. 1996 The National Information Infrastructure Protection Act (NIIPA)[95]
18. 1998 The Communications Assistance Law Enforcement Act (CALEA)[96]
19. 1998 The National Infrastructure Protection Center
20. 1999 The Gramm-Leach-Bliley Act[97]
21. 2000 The Children's Online Privacy Protection Act (COPPA)[98]

---

[79] 18 U.S.C. § 2510 (1988).
[80] 15 U.S.C. §§ 1681-1681t
[81] 20 U.S.C. § 1232g.
[82] 5 U.S.C. § 552a(4).
[83] 12 USC § 3401-3422.
[84] 15 U.S.C. § 1693.
[85] P.L. 98-632 § 2(b).
[86] 47 U.S.C. §§ 521-559 (1994).
[87] 18 U.S.C. §§ 2510-2521.
[88] Pub. Law 100-235, 101 Stat. 1725 §§ 2(a) & 3, ¶ 33,300 (1987). Section 3(3) designated the Act of March 3, 1901 (15 U.S.C. §§ 271-278h) as the National Bureau of Standards Act and assigned to the National Bureau of Standards (NBS) the mission of developing standards, guidelines, and associated methods and techniques for computer systems. The Act was renamed the National Institute of Standards and Technology Act, and the NBS was retitled the National Institute of Standards and Technology by Pub. L. 100-418 § 511(a)(2)(the Omnibus Trade and Competitiveness act of 1988).
[89] 18 U.S.C. § 2710.
[90] Computer Matching and Privacy Protection Act Amendments of 1989, Pub. Law 101-56, 103 Stat. 149 (1989).
[91] 47 U.S.C. § 227
[92] Full text can be found at http:// www.eoic.org/crypto/kepy-escros/white-paper.html.
[93] 18 U.S.C. § 1030 (1994).
[94] Pub. L. No. 104, § 222, 110 Stat. 56 (1996).
[95] Pub. L. No. 104-294 (1996) (available at http://thomas.loc.gov); 18 U.S.C. § 1030(a)(2) (1996).
[96] 47 U.S.C. § 1001, available at htttp://www.techlawjounal.com/agencies/calea/47USC1001.htm>.
[97] Pub. L. No 106-102, 113 Stat. 1338 (1999).

FTC Action Under the Unfair or Deceptive Trade Practices Act. While the political climate calls for self regulation in the electronic transmissions industry, the FTC has been bringing actions under the Federal Trade Commission Act (FTCA)[99] This act gives it the power to take enforcement action against site owners who do not follow the privacy practices they have advertised on their own websites.[100]

---

[98] 15 U.S.C. §§ 6501-6506.

[99] *Id*. § 41.

[100] *In re Geocities, Docket* No. C-3849 (Final Order Feb. 12, 1999, consent agreement (at <<http://www.ftc.gov/os/1999/9905/lbtord.htm>>) the FTC filed a complaint against Geocities, Inc. alleging that its failure to abide by the terms of its stated privacy policy constituted an unfair or deceptive act or practice within the meaning of section 5(a) of the FTC Act. Geocities offers its members free e-mail accounts, free and fee-based personal home pages, contests and children's clubs, among other services. People wishing to obtain free e-mail accounts, personal home pages or other services were required to complete a membership application that included both mandatory and optional information fields. The form also asked applicants to indicate whether they wished to receive "special offers" from advertisers and specific goods or services from individual companies. The FTC alleged that Geocities falsely represented that the personal identifying information it collected from membership application forms was used only to provide members specific advertising offers of goods or services requested. In fact according to the FTC, Geocities sold, rented, or otherwise disclosed this information to third parties to be used for purposes other than the ones for which permission had been obtained from Geocities members. Second, the FTC alleged that Geocities falsely represented that the "optional information" it collected from members was not disclosed to third parties without the member's permission. In fact, the FTC alleged that Geocities disclosed this information to third parties that used it to conduct targeted advertising to Geocities members. Third, The FTC alleged that GeoCities collected and maintained personal identifying information of children who signed up to join the Official GeoCities' GeoKidz Club or to participate in contests. In fact according to the FTC, such information was collected and maintained by third party "community leaders," who ran GeoCities' contests.

A consent judgment was entered in August 1998 prohibiting GeoCities from making any misrepresentation about its collection or use of personal identifying information from or about consumers, including what information would be disclosed to third parties and how the information would be used. GeoCities agreed to provide "clear and prominent notice" to consumers of its data collection practices. The Consent Judgment also contained specific requirements on how GeoCities' new privacy policy would be posted on its web site. GeoCities further agreed that it would not collect personally identifying information from any child age 12 or younger if it has actual knowledge that the child did not have the permission of a parent to provide such information. The judgment further provides that GeoCities shall not be deemed to have actual information where a child has falsely represented that she is an adult and it had no reason to doubt such information.