A COMPANY’S GUIDE TO AN EFFECTIVE WEB SITE PRIVACY POLICY

Quincy Maquet*

“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

--Alan Westin

Information privacy is “an individual’s claim to control the terms under which personal information--information identifiable to the individual--is acquired, disclosed, and used.”

--Information Infrastructure Task Force

I. INTRODUCTION

The recent growth of the Internet has provided businesses new and exciting opportunities to expand their business capabilities by using commercial Web sites. This growth has not only benefited businesses, but also the consumer. The Internet now provides the consumer with a wide variety of goods and services all at the click of a mouse. However, this convenience also has a very significant drawback for consumers: loss of privacy.


1 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Atheneum, 1967). Alan Westin is generally credited with the most well known definition of information privacy. See also ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971) (exclaiming that “the basic attribute of an effective right of privacy is the individual’s ability to control the circulation of information relating to him--a power that often is essential to maintaining social relationships and personal freedom.”); Charles Fried, Privacy, 77 YALE L.J. 475, 482 (1968) (stating “[p]rivacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.”); William A. Parent, Recent Work on the Concept of Privacy, 20 AM. PHIL. Q. 341, 346 (1983) (noting “privacy is the condition of a person’s not having undocumented personal information about himself known by others.”).

The ever-present use of computers to store personal information about individuals has given rise to increasing concerns about privacy. Many online businesses often sell a consumer’s personal information, such as buying habits, addresses, and credit card purchasing patterns, to direct marketing companies. Businesses obtain some of this information online through a variety of different means, e.g., registration pages, online contests and user surveys. However, much of the information obtained by commercial Web sites is without the user’s knowledge. This is done through a number of methods, including the use of persistent identifiers - better known as “cookies” -- stored on the user’s computer. Therefore, to help avoid unfair uses of the consumer’s personal information, every company’s Web site should contain a privacy policy.

A privacy policy is the first step to ensuring consumers against the misuse of their personal information. This policy should provide notice to the consumer about when personal data is collected, what data is collected, how it will be used and to whom it will be disclosed. A comprehensive privacy policy provided by a company on its Web site will allow the consumer to make an informed decision of whether to continue to use the Web site, and will create a greater trust in the electronic commerce infrastructure in this country and abroad.

This Comment examines many of the privacy concerns facing businesses seeking to create a commercial Web site. First, this Comment evaluates the various methods of data collection and addresses the various privacy concerns of consumers. Second, this Comment discusses the laws in the United States and abroad that attempt to regulate the gathering, transfer and use of an individual’s personal information. Next, this Comment scrutinizes the effectiveness of current self-regulation tactics used by businesses on the Internet, as well as the Information Infrastructure Task Force. Finally, this Comment drafts a privacy policy that companies seeking to establish a commercial Web site on the Internet should implement.

II. WEB SITES

The exponential growth of Web sites on the Internet has allowed businesses to connect to their target markets with much greater ease than in past decades. However, the increasing popularity of the Internet raises two distinct privacy concerns. First, the

---


5 However, other information comes from firms that specialize in providing personally identifiable information about individuals. These firms, called reference services, provide “‘one- stop shopping’ for anyone looking for information about a person.” See Kang, supra note 2, at 1294 n.207. See also ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 60 (1992) (explaining that a credit reporting company keeps “monthly tabs on 165 million consumers” and Wiland Services stores 1000 variables on 215 million individuals in its “ULTRAbase”).

6 In 1999, the Internet had more than 200 million users worldwide and linked more than 100 countries. Webopedia (visited April 4, 2000) <http:// www.webopedia.com>.
amount and accessibility of personal information on the Internet is greatly increased.\(^7\) Second, connectivity allows participants in an online environment to monitor and record an Internet user’s every move.\(^8\) Before evaluating how online companies are violating consumer’s privacy rights, one must understand the various business models operating on the Internet.

There are generally five business models that are employed on the Internet. These are:

1. the *Internet Presence Model*, which is used by businesses to raise consumer awareness of its name and products without any direct sales or advertising;

2. the *Advertiser Supported or Sponsored Model*,\(^9\) where advertising on the site is the sole source of revenue, content is offered for free and nothing is offered for sale;

3. the *Fee Based or Subscription Model*,\(^10\) which charges the users a fee before accessing content;

4. the *Efficiency or Effective Gains Model*, where a business uses the Web to decrease operating costs; and

5. the *Online Storefront Model*, which allows consumers to purchase goods or services directly over the Web site.\(^11\)

Irrespective of the business model a company employs, a company’s ability to attract and retain customers over time is essential for a successful Web site.\(^12\) Some experts have identified this factor as “traffic.”\(^13\) The best way to stimulate traffic on a company’s Web site is to offer some free content on its site.\(^14\) An additional factor many companies identify as essential for a successful Web site is “flow.”\(^15\) As one electronic commerce expert explained, “‘[f]low’ describes an online experience in which the user is completely engaged and focused while browsing or surfing the Web, has a sense of control over the experience, and has a proper mix of skills and challenges.”\(^16\) If a company is able to enhance the user’s flow experience, then the user will return to the


\(^8\) Id.

\(^9\) Id. Am. Civil Liberties Union, et al. v. Reno, 31 F. Supp. 2d 473, 486 (E.D. Pa. 1999). The Advertiser Supported or Sponsored Model is the most popular model, which many online magazines use. Id.

\(^10\) Id. The Fee Based or Subscription Model is the least popular of all models, even though some companies have been successful using this model, e.g., The Wall Street Journal Web site. Id.

\(^11\) Id.

\(^12\) Id. at 487.

\(^13\) Id.

\(^14\) Id.

\(^15\) Id.

\(^16\) Id.
Web site, and in turn, increase the traffic of the Web site. By establishing a sufficient amount of traffic, a company creates a broad range of customers from which it may collect personally identifiable information.

III. DATA COLLECTION

A company’s interest in an individual consumer is based on the information collected from the individual, either directly or indirectly, when the consumer visits the company’s Web site. Companies with a presence on the Internet will directly gather personal information - such as name, gender, address, age, income, lifestyle, hobbies, and interests - by using registration and other forms on its Web site. The use of registration and similar types of forms allows a consumer to voluntarily offer personal information about his or herself. However, many companies with a presence on the Internet often gather information indirectly, i.e., without the consumer volunteering the information. This time the gathering of this information is automatic and without the consumer’s awareness. The collection of this data is accomplished by either examining the “clickstream” data from the user’s electronic transmission, or more commonly by collecting “cookies.”

A. CLICK STREAM DATA

In addition to users directly providing information to Web sites, the electronic transmission itself leaves a “personal profile” usually without the user’s knowledge.

---

17 Id.
18 Oscar H. Gandy, Jr., Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 U. CHI. LEGAL F. 77, 106 (1996). New Web-monitoring services are analyzing the raw traffic statistics and turning them into useful marketing data, like determining how many times the same people viewed an ad and the route used to get to the ad. Id. at 111. Advertisers might also want to know the Web site people visited next, to determine additional Web sites the advertiser may use for advertising purposes. Id.
19 See ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION?: FROM PRIVACY TO PUBLIC ACCESS 3-4 (1995) (stating that “[a] great deal of information we consider to be highly personal ... is now being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. These transactions usually take place without our knowledge or consent.”). Electronic periodicals, such as Wired Magazine’s electronic alternative, HotWired, require users to register a user name and password, as well as a unique identifier. See Gandy, supra note 18, at 111. This allows the Web site to link individuals with their informational choices. Id.
20 Id. at 106. Some commercial firms provide software that analyzes data generated by visits to an organization’s server. Id. While there are still difficulties in establishing the unique identity of individuals who visit a site, such identification “would make the Web the best measured of all commercial media.” Id. at 110-11.
21 Joshua B. Sessler, Comment, Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet, 5 J.L. & POL’Y 627 (1997). A “Personal Profile” is an electronic “footprint” similar to the information a telephone call conveys to the telephone company. Id. The telephone company receives information about the length, origin and destination of a telephone call, but nothing about the content of the call. Id. at 677 n.9. This is similar to a “personal profile” because the server can track the pages a user views, the length of time spent on each page, and what page the user went to next, but is unable to determine what content the user viewed while on these pages.

2 Chi.-Kent J. Intell. Prop. 1
This “imprint” is referred to as “transaction generated information” (“TGI”) 24 or “clickstream” data 25—which means it can track each page a user views. Each time a user visits a Web site, the server typically logs the transaction. 26 Using this information, a server can track the “clickstream” of a user by sequence, time and duration. 27 Servers maintain clickstreams in one of two ways. The server can use the IP addresses and other information in its log and try to match them to their time-stamps. 28 Or, more easily, the server can set a ‘cookie.’ 29

B. COOKIES

Many Web sites collect “cookies.” 30 A cookie is information about a Web site visit, which the Web browser receives from the Web site 31 and stores on the user’s hard drive. 32 The Web site is then able to “read” the information during each successive visit to the Web site by the user. This information includes the user’s Internet Service Provider (ISP), type of hardware and software used during the visit, the Web site linked from, as

\[\text{Eq. 1}\]

23 Jim Erickson, Are Those Who Go Online to Send Junk Mail Out of Line?, STAR TRIB., June 30, 1996, at 3D. This information is used to organize data regarding Internet usage patterns that is eventually packaged and sold for marketing purposes—all without the user’s knowledge or consent. Larry Irving, Safeguarding Consumer’s Interests in Cyberspace, 1996 U. CHI. LEGAL F. 1, 7 (1996).

\[\text{Eq. 2}\]

24 See BRANSCOMB, supra note 19, at 48. “TGI” is transmission-related because it merely summarizes the electronic transmission itself. Sessler, supra note 22, at 631. This information is retrievable and may be used by marketing companies who claim that they will be “better able to target a particular consumer’s preferences or interests.” Id. at 631-2. Other uses of TGI are new visitor counting, behavior tracking and self-configuring Web pages. Id. at 640.

\[\text{Eq. 3}\]

25 Susan E. Gindin, Lost and Found in Cyberspace: Information Privacy in the Age of the Internet (visited September 20, 1999) <http://info-law.com/lost.html>. A “clickstream” has been defined as “the database created by the date-stamped and time-stamped, coded/interpreted, button-pushing events enacted by users of interactive media controlling the systems via alphanumeric PC keyboards, mice, and similar devices.” Id.

\[\text{Eq. 4}\]

26 Kang, supra note 2, at 1294 n.328. Standard Web logs record identity information. This information includes: (1) the IP address and domain name, (2) the username if the user is authenticated, (3) the login name if the identified program is running on both client and server, (4) the time and date of the request, (5) the URL of the requested resource, (6) the byte length of the resource, (7) the referrer variable, i.e., the URL of the resource from which the request was made, and (8) the user-agent variable. Id.

\[\text{Eq. 5}\]

27 Online service providers track the navigational patterns of their users in order to make improvements in the services that they offer to customers. America Online, in its terms of service, explains that it records user’s “navigational and transactional” information to “understand our member’s reactions to menu items, content, services and merchandise offered through AOL and to customize AOL based on the interests of our members.” AOL Homepage, (visited September 30, 1999) <http://www.aol.com>.

\[\text{Eq. 6}\]

28 Interestingly, if a person clicks on a link returned by a search engine, the server that person goes to--by examining the referrer variable--can determine the search engine used, as well as the keywords used in the query. See Kang, supra note 2, at 1294 (noting that the referrer variable is the URL of the resource from which the request was made).

\[\text{Eq. 7}\]

29 Id. at 1227.

\[\text{Eq. 8}\]

30 One commentator compared cookies to the notion of “a store being able to tattoo a bar code on your forehead, and then laser-scan you every time you come through the doors.” See Sessler, supra note 22, at 633.

\[\text{Eq. 9}\]

31 However, many browsers already allow individuals greater control over the setting of cookies. For example, Netscape’s Navigator 4.0 allows a person to set preferences to accept all cookies, reject all cookies or warn the individual whenever cookies are set. Kang, supra note 2, at 1294 n.152.

\[\text{Eq. 10}\]

32 Generally, cookies do not pose a threat to either destroy or compromise a system. Myrna L. Wigod, Privacy in Public and Private E-mail and On-line Systems, 19 PACE L. REV. 95, 100 (1998).
well as which files the user accessed and the amount of time spent on each page. This information permits Web sites to learn what visitors like and dislike about the site, and to personalize the site to allow users to select options used during previous visits automatically.

The information that cookies collect from users may be profitable both to electronic commerce companies and data collection agencies. Thus, whether the convenience of cookies outweighs the loss of privacy is an issue that privacy advocates and Internet users worldwide constantly debate, and has led many consumers to have serious concerns about a loss of privacy when navigating through the Internet.

IV. CONSUMER CONCERNS ABOUT WEB SITE DATA COLLECTION

There are various privacy groups, such as CAUCE and EPIC which have been established to advocate the privacy rights of consumers. These groups conduct various studies and surveys that address the growing privacy concerns of consumers online. In addition to these groups, AT&T recently released its findings from a survey conducted in

---

33 Kang, supra note 2, at 1228. However, a user’s computer does not serve up cookies simply to anyone who asks. In other words, not all servers have access to all cookies. When each cookie is initially set, it delineates the range of servers to whom the cookie may be subsequently given. Id. The domain name of the server that initially set the cookie is the default range. Id. Thus, if the server chicagoinfo.movietime.com set a cookie identifying my zip code as 60606, but did not specify a domain name range, then, by default, the cookie will only be given to chicagoinfo.movietime.com in the future. Id. Although chicagoinfo.movietime.com can set the domain range to a larger set of servers by including the domain name range on the tail of its name, movietime.com, it cannot set the range to an entirely different domain name, movietime.com. Id. Therefore, the user’s computer will only disclose a cookie if the domain name range for the cookie matches the tail name of the server’s domain name. Id. Put simply, a cookie with the domain name range movietime.com will not be disclosed to any server that has the tail of firstvideo.com. Thus, only the companies that set the cookie initially can usually read its cookies. Id.

34 Gindin, supra note 25, at <http://infolaw.com/lost.html>. For example, many Web servers provide movie listings by zip code. Due to the inefficiency of requiring a user to reenter his zip code at each visit, the server saves the zip code and other information in a cookie on the user’s hard drive. Kang, supra note 2, at 1227. During each subsequent visit, the server can access the cookie and automatically provide local movie news without asking the user for his location. Id.

35 Id. Usually, the information contained in a cookie does not identify a specific individual. Gindin, supra note 25, at <http://infolaw.com/lost.html>. However, when combined with on-site registration data, cookie data may be used to build a profile of a specific user. Id. Many Web sites require on-site registration, including name, physical address and email address in order for a user to obtain access or certain benefits. Id.

36 Timothy J. Walton, Internet Privacy Law (visited September 28, 1999) <http://www.netatty.com/privacy.html>. America OnLine has been accused of selling information about its users. Id. Additionally, the Federal Trade Commission found that GeoCities, a Web site where users input personal information, was selling user information in violation of its own privacy policy. See In the Matter of GeoCities, FEDERAL TRADE COMMISSION (Aug. 13, 1998). This has led many cookie proponents to call for the reduction in the amount of information that cookies collect.

37 CAUCE, the Coalition Against Unsolicited Commercial Email is a volunteer organization to advocate for a legislative solution to the problem of unsolicited e-mail. See CAUCE Homepage (visited April 20, 2000) <http://www.cauce.org>.

38 EPIC, the Electronic Privacy Information Center, is a public interest research center established in 1994 to focus attention on the protection of privacy, the First Amendment, and constitutional values. See EPIC Homepage (visited April 18, 2000) <http://www.epic.org>.
November of 1998 that attempted to gain an understanding of the privacy concerns of Web users. This survey targeted heavy Internet users, and provided the following major findings: (1) Internet users are more likely to provide information when they are not identified; (2) some types of data are more sensitive than others; (3) many factors are important in decisions about information disclosure; (4) acceptance of the use of persistent identifiers, i.e., “cookies,” varies according to their purpose; and (5) a joint program of privacy policies and privacy seals seemingly provides a comparable level of user confidences as that provided by privacy laws. Therefore, companies should examine the first four of the above findings, and provide consumers with a privacy policy and seal to enhance the level of consumer confidence in the company’s Web site.

A. CONSUMERS PREFER NOT TO BE IDENTIFIED WHEN PROVIDING INFORMATION ON THE INTERNET

The AT&T survey provided the respondents with two scenarios. The first scenario involved a banking Web site, and the other was a news, weather and sports Web site. In each of these scenarios, the Web site requested information either with or without personally identifiable information. In the first scenario, fifty-eight percent of the respondents explained that “they would provide information about their income, investments and goals in order to receive customized investment advice.” However, only thirty-five percent of these respondents would provide the same information when coupled with personally identifiable information.

In the second scenario, the news, weather and sports Web site, eighty-four percent of the respondents explained that “they would provide their zip code and answer questions about their interests in order to receive customized information.” Similar to the banking Web site however, only forty-nine percent of the respondents would provide the same information if they were required to include their name.

Both of the scenarios above provided the respondents a service without a fee. However, when a Web site requests personal information, a significant portion of the

39 LORRIE FAITH CRANOR ET AL., BEYOND CONCERN: UNDERSTANDING NET USERS’ ATTITUDES ABOUT ONLINE PRIVACY, AT&T LABS-RESEARCH TECHNICAL REPORT 99.4.3 [hereinafter AT&T SURVEY] (visited September 10, 1999) <http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm>. This study was one of the first studies conducted regarding consumer privacy online, and has been referenced by various consumer privacy organizations, such as Truste. See Truste Homepage (visited April 20, 2000) <http://www.truste.com>.


41 Id. Additionally, the survey also found that: (1) Internet users dislike automatic transfer, and (2) Internet users dislike unsolicited communications. Id. However, this Comment will only address the five major findings mentioned in the text.

42 Id.
43 Id.
44 Id.
45 Id.
46 Id.
respondents report concerns over the loss of privacy. This concern is a direct result of the consumer’s awareness of the potential collection and misuse of this personal information. Therefore, Web sites must establish the trust of the consumer and guarantee customers that this information will not be misused.

B. THE SENSITIVITY OF DATA VARIES AMONG CONSUMERS

The AT&T survey asked their respondents how comfortable they were with: (1) providing twelve specific pieces of information to Web sites, and (2) a child in their care between the ages of eight and twelve providing the same information. Very few of the respondents said they would usually feel comfortable providing their medical information (18%), credit card number (3%) or social security number (1%). However, a large number of the respondents usually or always felt comfortable providing their email address (76%) and their age (69%). Respondents were noticeably less comfortable allowing a child to provide this same information.

The AT&T report also notes that consumer awareness of the problems associated with divulging different types of information affects their level of concern. Publicity surrounding identity theft and credit card fraud has raised awareness about the dangers of social security numbers and credit card numbers falling into the wrong hands. However, there has been less publicity about the dangers associated with the disclosure of medical records. This lack of publicity may account for the fact that the respondent’s concern about divulging credit card and social security numbers is significantly higher than that for medical records—which arguably are just as sensitive.

C. CONSUMERS CONSIDER MANY FACTORS WHEN DISCLOSING THEIR INFORMATION

The sharing of information with other companies was the most important factor that respondents considered when determining whether to disclose information to a Web site. Three other factors of importance to respondents also emerged: (1) whether the Web site identifies how it uses the information it gathers; (2) the kind of information collected, e.g., personal or sensitive; and (3) the purpose for which the information is collected. In addition to these three factors, the respondents also rated other factors as very important regarding the disclosure of their personally identifiable information. These factors include: (1) whether a Web site is run by a trusted company or organization; (2) whether a Web site will allow people to find out what information about

47 Id.
48 Id. Not surprisingly, none of the respondents said they were always comfortable providing their credit card number or social security number. Id.
49 Id.
50 Id. Very few of the respondents said they were always or usually comfortable with a child providing their email address (16%) and their age (14%). Id.
51 Id.
52 Id.
53 Id.
54 Id.
them is stored in their databases; and (3) whether the Web site will remove someone from their mailing lists upon request.\textsuperscript{55}

**D. ACCEPTANCE OF THE USE OF PERSISTENT IDENTIFIERS VARIES ACCORDING TO USE**

Many Internet users are concerned that their online activities are being tracked over time. Such tracking can be accomplished by using persistent identifiers, \textit{i.e.}, “cookies,” stored on a user’s computer. When asked, fifty-two percent of the respondents indicated they were concerned about cookies, while another twelve percent said they were uncertain about the definition of a cookie.\textsuperscript{56} Of those who knew what cookies are, fifty-six percent said they had changed the cookie settings on their Web browser to prohibit accepting all cookies without warning.\textsuperscript{57}

After posing several scenarios with Web sites using persistent identifiers, the AT&T survey concludes that most respondents were not opposed to the use of persistent identifiers.\textsuperscript{58} However, the report noted that many people have misconceptions about these technologies and concerns about some of their uses.

**V. LAWS GOVERNING THE COLLECTION OF PERSONAL INFORMATION**

Today, there are specific federal privacy laws dealing with videotape rental records,\textsuperscript{59} credit reports,\textsuperscript{60} political contributors,\textsuperscript{61} tax records,\textsuperscript{62} cable television viewing habits\textsuperscript{63} and the delivery of pandering materials through the mail.\textsuperscript{64} However, as the Internet expands, current laws often do not apply to this new context. Therefore, Congress is introducing new bills that are aimed directly at Internet privacy.\textsuperscript{65} These bills include: the \textit{Online Privacy Protection Act of 2000},\textsuperscript{66} the \textit{Consumer Internet Privacy

\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
\textsuperscript{65} In addition to the federal bills that are being introduced, many states are introducing bills that are aimed at protecting a consumer’s privacy on the Internet. Minnesota for example, has introduced a bill that requires the development of an online privacy notice by public and private entities with a presence on the Internet. H.B. 3731 (MN 1999). This bill also places restrictions on the use and dissemination of personal information. Id. New York has also introduced legislation that requires state agencies and companies within the state to adopt Internet privacy protection policies that address notice, consent, participation and security. A.B. 8130 (NY 1999). Finally, Wisconsin is currently debating a bill that would prevent companies using Web sites from disclosing personal information about state residents gathered through the Web site. S.B. 375 (WI 1999). See also H. B. 2717 (AZ 2000) (regulating the practices of “information custodians”); Exec. Order No. 51 (VA 1998) (requiring the state to develop uniform guidelines for privacy policies for Web sites).
\textsuperscript{66} H.R. 3560, 106\textsuperscript{th} Cong. (1999).
Copyright © Chicago-Kent Journal of Intellectual Property

Protection Act of 1999,67 and the Personal Data Privacy Act of 1999.68 Additionally, Congress has already enacted general privacy laws such as the Electronic Communications Privacy Act of 1986,69 the Privacy Act of 1974,70 and the Children’s Online Privacy Protection Act of 199871 to protect consumer privacy on the Internet.

A. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

The Electronic Communications Privacy Act of 1986 (ECPA)72 amended the 1968 federal wiretap law73 to protect previously unprotected forms of electronic communications.74 The ECPA provides a uniform basis for the circumstances in which Internet service providers may disclose user information to the government.75 However, the ECPA is limited because it does not prohibit disclosure of user information to non-governmental entities.

Under the ECPA, a governmental entity must obtain a warrant or court order to obtain information from an online service provider about one of its users.76 In McVeigh v. Cohen,77 the Navy sought to review a sailor’s email and contacted his online service provider for his customer profile. However, the Navy failed to provide the service provider with a warrant or court order to obtain this information. Therefore, a United States District Court found that the Navy violated the ECPA for failing to obtain the required documentation for obtaining this personal information.78 In addition to the ECPA, the government has also enacted the Privacy Act of 197479 to shield consumers from an invasion of privacy.

B. PRIVACY ACT OF 1974

The Privacy Act of 197480 seeks to limit the collection of personal information from individuals. Similar to the ECPA however, the Privacy Act relates to governmental

74 18 U.S.C. § 2510 (1998). The ECPA covers all forms of digital communications, including data transmissions between computers, paging devices, email and video transmissions, and prohibits unauthorized eavesdropping by all persons and businesses. Id. Additionally, the ECPA prohibits the interception of electronic messages as well as the unauthorized access to messages stored on a computer system. Id.
78 Id. at 222.
80 See id.
conduct instead of the behavior of private entities.\textsuperscript{81} The Privacy Act seeks to strike a balance between the government’s need to gather and use personal information and the individual’s privacy interest in controlling this information. Under the Privacy Act, federal agencies are allowed to maintain records containing only the amount of information about an individual that is essential to accomplish the agency’s purpose.\textsuperscript{82} Additionally, the agency must maintain this information accurately and completely, and they must collect the information directly from the individual if possible.\textsuperscript{83}

The Privacy Act further requires every federal agency that maintains a system of records to: (1) permit the individual to control disclosure of the information in the record;\textsuperscript{84} (2) retain records of the information that is disclosed;\textsuperscript{85} (3) permit the individual to review and have a copy of the information in the record;\textsuperscript{86} and (4) allow the individual to request an amendment to the information in the record.\textsuperscript{87} However, as mentioned previously, the Privacy Act regulates information retained by government entities, but not private entities. Thus, many of the private data collection agencies on the Internet are not governed by these requirements.

C. CHILDREN’S ONLINE PRIVACY PROTECTION ACT OF 1998

In July 1997, the Federal Trade Commission (FTC) investigated the advertising practices of KidsCom, an interactive Web site targeted at children ages 4 to 15.\textsuperscript{88} KidsCom is a Web site that collected data from its minor users related to their preferences about specific products, and then provided this information to private companies.\textsuperscript{89} In response to this investigation, the FTC issued an open letter regarding the advertising practices of KidsCom. In its letter of finding, the FTC set out guidelines regarding the collection of personal information from children:

1) It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (\textit{i.e.}, participating in a quiz) when the information will also be used for another purpose (\textit{i.e.}, marketing) which parents would find material, absent a clear and prominent disclosure to that effect;

2) Any disclosure regarding the collection and use of children’s personally identifiable information must be made to the parent; and

3) An adequate notice to parents should disclose: who is collecting the

---

\textsuperscript{81} See id.
\textsuperscript{82} See id. at § 552a(e)(1).
\textsuperscript{83} See id. at § 552a(e)(2).
\textsuperscript{84} See id. at § 552a(b).
\textsuperscript{85} See id. at § 552a(c).
\textsuperscript{86} See id. at § 552a(d)(1).
\textsuperscript{87} See id. at § 552a(d).
\textsuperscript{89} Id.
personally identifiable information, what information is being collected, its intended uses, to whom and in what form it will be disclosed to third parties, and the means by which parents may prevent the retention, use or disclosure of information.\textsuperscript{90}

Consequently, the \textit{Children’s Online Privacy Protection Act of 1998} was eventually enacted to regulate the collection of personal information from children online.\textsuperscript{91} This Act requires online companies to obtain parental permission before soliciting information from children under the age of 13.\textsuperscript{92} The Act protects the following information: first and last name, home or other physical address, email address, telephone number, social security number, or any other information that would enable the information seeker to locate or contact an individual.\textsuperscript{93} Additionally, the Act requires commercial Web sites to get parental consent for the collection, use or disclosure of any personal information from children.\textsuperscript{94}

\textbf{D. PENDING LEGISLATION RELATING TO THE COLLECTION OF PERSONAL INFORMATION}

Due to the increasing concern about consumer privacy on the Internet, Congress is presently debating various bills that offer greater protection to consumers on the Internet. The \textit{Online Privacy Protection Act of 2000},\textsuperscript{95} would require the FTC to delineate regulations to protect the personal information collected from consumers who are not covered by the \textit{Children’s Online Privacy Protection Act of 1998}.\textsuperscript{96} Additionally, this bill would provide consumers with greater control over the collection and use of their personal information over the Internet.\textsuperscript{97}

The \textit{Consumer Internet Privacy Protection Act of 1999}\textsuperscript{98} seeks to regulate the personal information provided by subscribers to interactive computer services.\textsuperscript{99} It contains three basic provisions: (1) an interactive computer services cannot disclose personally identifiable information without written consent, (2) it cannot falsify information if it does disclose, and (3) individuals have the right to access the information kept on them.\textsuperscript{100}

Lastly, the \textit{Personal Data Privacy Act of 1999}\textsuperscript{101} is not limited to the Internet, but

\textsuperscript{90} Id.
\textsuperscript{92} \textit{See id.}
\textsuperscript{93} \textit{See id.} at § 6501.
\textsuperscript{94} \textit{See id.} at § 6502.
\textsuperscript{95} S.B. 809, 106\textsuperscript{th} Cong. (1999).
\textsuperscript{96} \textit{See id.}
\textsuperscript{97} \textit{See id.}
\textsuperscript{98} H.R. 313, 106\textsuperscript{th} Cong. (1999).
\textsuperscript{99} \textit{See id.} The bill reads: “An interactive computer service shall not disclose to a third party any personally identifiable information provided by a subscriber to such service without the subscriber’s prior informed written consent.” \textit{See id.}
\textsuperscript{100} \textit{See id.}
\textsuperscript{101} H.R. 2644, 106\textsuperscript{th} Cong. (1999).
would have an immediate impact for online data collectors.\footnote{See id.} This bill would prohibit disclosure of personal data\footnote{See id.} by private businesses and government entities without written consent.\footnote{See id.} Additionally, the bill would require entities to provide individuals with access to their information within five days, as well as provide a yearly report to the individual on their personal data.\footnote{See id.}

\section*{E. POTENTIAL TORT CLAIMS}

In addition to the statutes mentioned above that focus primarily on regulating the government, the right to privacy has also emerged through common law tort litigation. While much recognition is given to the scholarly arguments of Warren and Brandeis - considered the founders of privacy tort law,\footnote{Warren and Brandeis are considered the founders of privacy tort law based on their article The Right to Privacy, 4 HARV. L. REV. 193 (1890).} the Restatement (Second) of Torts delineates the cognizable claims for invasion of privacy. These formulations for invasion of privacy taken in a cyberspace context are: (1) unreasonable intrusion upon the seclusion of another; (2) unreasonable publicity given to another’s private life; and (3) publicity that unreasonably places another in a false light before the public.\footnote{Restatement (Second) of Torts § 652A (1976). Additionally, the Restatement also discusses a fourth claim for invasion of privacy: the appropriation of another’s name or likeness. Id. However, this claim will probably not be brought in a cyberspace context, and thus will not be discussed in this Comment.}

\subsection*{1. Unreasonable Intrusion Upon the Seclusion of Another}

Traditionally, intrusion arises from the physical or visual intrusion into the personal or private “space” of another.\footnote{See Dietemann v. Time, 449 F.2d 245 (9th Cir. 1971); Miller v. NBC, 187 Cal. App. 3d 1463 (1986).} It usually arises where one has improperly spied upon, taped or entered the home of another without consent.\footnote{Id.} In cyberspace, intrusion claims will be the result of cyberspace intrusions, such as “hacking.” Hacking conduct occurs when a person intercepts a communication intended for another, or when an individual breaks into another’s system without authorization. Using this method, many hackers obtain personal information about others, and then sell this information or use it in other improper ways.

\subsection*{2. Unreasonable Publicity Given to Another’s Private Life}

An individual invades another’s privacy when he or she publicly discloses private
facts about the person, that a reasonable person would consider highly offensive.\textsuperscript{110} Family, sexual, medical and financial facts are all usually considered private facts under this tort. In defense of this claim, many individuals claim that the information disclosed is newsworthy and thus not actionable. The general criteria for determining newsworthiness are: (1) the social value of the facts published; (2) the depth of intrusion into ostensibly private affairs; and (3) the extent to which the individual voluntarily acceded to a position of public notoriety.\textsuperscript{111} Although these claims may not be as prevalent as other tort claims, i.e., defamation, these claims may increase due to the growth of the Internet, as well as Internet operators who lack the legal knowledge necessary to prevent these claims.

3. Publicity That Unreasonably Places Another in a False Light Before the Public

False light claims usually arise where a false impression results from something other than an express statement. A frequent example of a false light claim arises when a picture and an unrelated statement are placed in close proximity, giving rise to the impression that the statement and the picture coincide.\textsuperscript{112} Although much of the information on the Internet is considered public information, and thus unactionable under the above mentioned tort claim, the disclosure of this information coupled with a picture that does not coincide with the information, may allow individuals to actively pursue a false light claim.

F. EUROPEAN UNION PRIVACY DIRECTIVE

Privacy concerns on the Internet accelerated when the European Union implemented its Data Privacy Directive (“Directive”).\textsuperscript{113} The Directive establishes new European-wide\textsuperscript{114} standards for the gathering, use and disclosure of personal information.

The Directive attempts to protect all personal data\textsuperscript{115} that is processed\textsuperscript{116} by automatic means or that is processed manually, but form or intend to form part of a filing system or database of personal information.\textsuperscript{117} Specifically, member countries are required to adopt legislation requiring that personal data must be: (1) “processed fairly and lawfully;” (2) “collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;” (3) “adequate,

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{111}Briscoe v. Reader’s Digest Assoc., Inc. 4 Cal. 3d 529, 541 (Cal. 1971).
\item \textsuperscript{112}Kapellas v. Kofman, 1 Cal. 3d 20 (1969).
\item \textsuperscript{113}See COUNCIL DIRECTIVE 95/46/ED ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, 1995 O.J. (L 281) [hereinafter DIRECTIVE].
\item \textsuperscript{114}The Member countries subject to the European Convention are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom. Each member country must assign “one or more public authorities” to monitor industry compliance with the legislation or regulations adopted pursuant to the Directive. See id. at art. 28.
\item \textsuperscript{115}“Personal data” is broadly defined in the Directive to include all information that relates to an identified or identifiable individual. See id. at art. 2.
\item \textsuperscript{116}See id. “Processing” of data refers to any operation performed on such data, such as collecting, storing, recording, altering, retrieving, organizing or disclosing it. See id.
\item \textsuperscript{117}See id. at art. 3.
\end{itemize}
\end{footnotesize}
relevant and not excessive in relation to the purposes for which they are collected;” (4) “accurate and kept up to date;” and (5) “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.”

Additionally, data may only be collected and processed in a limited set of circumstances, including where: (1) the individual “has unambiguously given his consent” to such processing; (2) “processing is necessary for the performance of a contract” to which the individual is or will become a party; (3) the processing is necessary for “compliance with a legal obligation;” or (4) the processing is necessary to protect the “vital interests” of the person to whom the data pertains. Unless the individual to whom the data pertains already has the information, the individual must also be informed of: (1) the purpose of the processing for which the data is intended; (2) the existence of the right to review and correct this personal data; and (3) whether responses to questions seeking personal data are obligatory or voluntary, as well as the consequences for failure to respond.

The Directive has direct implications for companies operating in the United States. Article twenty-five of the Directive prohibits the transfer of personal data to a third country unless that country ensures an adequate level of protection for the personal data. Due to the lack of legislation in the United States governing information privacy, many companies within the United States may be unprepared to meet this standard of protection for personal data. Therefore, the Directive will prohibit data transfers between these companies and companies located within the member countries of the European Union.

V. SELF REGULATION

On July 13, 1999, the Federal Trade Commission released a report that recommended against any legislation to regulate online privacy. Therefore, companies should participate in the many extra-legal options available, such as “self-regulation,” to protect the privacy rights of their customers. Self-regulation can take the form of explicit codes of company conduct, actual contracts with consumers or consumer information privacy policies.

A. THE INFORMATION INFRASTRUCTURE TASK FORCE

---

118 See id. at art. 6. The Directive allows member countries to exclude from the scope of implementing legislation or regulations the processing of personal data gathered in connection with state security, defense, public security, important state financial interest, regulatory functions relating to the foregoing, and criminal and ethical investigations. See id. at art. 3.
119 See id. at art. 7.
120 See id. at art. 10.
121 See id. at art. 29.
123 See Mary G. Jones, Privacy: A Significant Marketing Issue for the 1990’s, 10 J. PUB. POL’Y & MARKETING 131, 133 (1991) (stating that American Express and Chase Manhattan have strict company policies that prohibit the disclosure of customer information to third parties).
The Clinton Administration created the Information Infrastructure Task Force (IITF) to address many of the policy issues arising in cyberspace. The IITF consists of representatives from various federal agencies who are experts in information and technological issues. 124 Of the three committees established by the IITF—Telecommunications Policy, Information Policy, and Applications and Technology—the Information Policy Committee is the most active in the pursuit for Internet privacy. Within that committee are two working groups: the Intellectual Property Working Group and the Privacy Working Group. 125 The Privacy Working Group’s efforts have generated much academic and political attention.

The IITF Principles, a central privacy document produced by the Privacy Working Group, has been adopted by the IITF and endorsed by the Office of Management and Budget. 126 These principles provide participants in the National Information Infrastructure (NII) guidance on the use of personal information. In this document, the IITF adopted the following general principles:

1. Personal information should be acquired, disclosed, and used only in ways that respect an individual’s privacy.
   a) Personal information should not be improperly altered or destroyed.
   b) Personal information should be accurate, complete and relevant for the purpose for which it is provided and used.

2. Information users should:
   a) Assess the impact on privacy when deciding whether to acquire, disclose or use personal information.
   b) Acquire and keep only information reasonably expected to support current or planned activities.

3. Information users . . . should provide adequate, relevant information 127 about . . . why they are collecting information; . . . what the information is expected to be used for; . . . what steps will be taken to protect [it]; . . . consequences of providing or withholding information; and . . . any rights of redress.

4. Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.

---

125 Id.
127 “What counts as adequate, relevant information . . . depends on the circumstances surrounding the collection of information.” Id.
5. Information users should not use personal information in ways that are incompatible with the individual’s understanding of how it will be used.\footnote{Id.}

These principles acknowledge that by its very nature, the electronic medium will shape privacy policies. Therefore, although these principles do not have legal effect, they are meant to “guide all NII participants as well as those who are drafting legislation and creating policy regarding the use of personal information.”\footnote{Id.}

\section*{B. \textsc{The Truste Program}}

The Electronic Frontier Foundation, a San Francisco-based Internet watchdog organization, is starting a worldwide campaign that allows Web sites to reveal their privacy policies via different “trustmarks.”\footnote{The TRUSTe On-Site Information Page (visited September 20, 1999) < http://www.etrust.com>.

\footnote{Id.}} This program, known as TRUSTe, informs users whether Web sites collect personal information, and if so, whether it will be released to third parties.\footnote{Id.}

TRUSTe has three tiers from which program participants can choose: (1) No Exchange - “insures anonymous usage, anonymous transactions, anonymous chat and anonymous tracking;” (2) One to One Exchange - ensures “that the services will not disclose individual or transactional data to third parties;” or (3) Third Party Exchange - “informs the user that the services will be disclosing information to third parties.”\footnote{Id.} Depending on which tier it chooses, a member of the TRUSTe program may display the appropriate “trustmark” on its Web site to indicate how it uses the consumer data gained through the site.\footnote{Id.} This trustmark allows consumers to make informed decisions about whether they wish to continue visiting a Web site where their personal information may not be secure.\footnote{Id.}

\section*{VI. PRIVACY POLICY REQUIREMENTS FOR A COMMERCIAL WEB SITE}

\textit{“The first rule of business is to establish the trust of the subscriber ...”}\footnote{INTERACTIVE SERVICES ASSOCIATION, GUIDELINES FOR ONLINE SERVICES: THE RENTING OF SUBSCRIBER MAILING LISTS (June 1995).}

Every commercial Web site on the Internet should have a privacy policy to ensure its users that the site will not compromise their privacy. This privacy policy should be
easy for users to find, read and use to make informed decisions about the collection and use of their personal information.

In June of 1998, the FTC issued a comprehensive report entitled “Privacy Online: A Report to Congress,” analyzing a survey that it conducted of over 1,400 commercial Web sites. The survey revealed that over eighty-five percent of these Web sites collected personal information from their customers. Furthermore, only fourteen percent of the Web sites surveyed provided notice to the customer of their collection of personal information, while only two percent provided a comprehensive privacy policy. After examining the results of the survey, the FTC found that self-regulation has yet to be established and that additional incentives are required to ensure that consumer privacy is protected and self-regulation is effective.

The FTC concluded in its report that there are four necessary elements to protecting consumer privacy: (1) notice to consumers about how personal information collected online is used; (2) choice for consumers about whether and how their personal information is used; (3) security of personal information; and (4) access for consumers to their own personal information to ensure accuracy. Following these elements, a company can draft a Web site privacy policy that will establish the trust of its users and protect these users from an invasion of their privacy.

A. CONSUMER NOTICE

Any privacy policy should be visible and readily available to the consumer on a company’s Web site. A company should write its policy in clear and easy-to-understand language and make the policy available before requesting personal information from users.

The privacy policy should cover all activities that the Web site makes available to the consumer, and should contain a broad definition of “protected information” to this effect. Due to consumer concerns about identity theft, “personally identifying information” such as social security numbers, prior and current addresses and birth dates should all be included under the definition of protected information. In addition to this information, the policy should also define all relevant terms, including the company’s collection, retention and dissemination of this information.

The privacy policy should also explain to consumers what information is being collected, which specific group it is collected from and how it is collected. Included in this portion of the policy, companies should advise consumers whether they use “cookies” after the consumer’s initial visit to the site, and whether the company releases this information to third parties.

---

137 Id.
138 Id.
139 Id.
The company must address children’s privacy in its policy as well. Due to the increased concern over this information, the policy should state that it will not at any time collect information from children. If however, a company seeks to create an interactive children’s Web site and collect this information, then it must clearly state that it is in accordance with the Children’s Online Privacy Protection Act of 1998.

Once a company informs consumers about how it collects information on its Web site, the company should make this collected information accessible to the consumer. This section of the policy should inform the consumer that they have the right to know what information the company has obtained about them, as well as the procedure for reviewing and correcting this information. This enables the company and the consumer to correct incomplete or inaccurate information that may have been obtained while navigating through the company’s Web site.

B. CONSUMER CONTROL AND CHOICE

A company’s privacy policy should also allow the consumer a choice of whether or not to allow the Web site to collect personal information. This is done by using an “opt-in” or “opt-out” method. Many companies prefer the “opt-out” method where the Web site can collect information unless the consumer takes an affirmative step to exclude his or herself from the collection of this information. However, consumers prefer the “opt-in” method because it allows greater control over their personal information. The “opt-in” approach is based on the assumption that consumers do not want to offer their information to the Web site, and thus, is more consistent with consumer control. Under this approach, the consumer has the choice to protect their personal information, or offer this information in return for benefits that the Web site offers.140

C. THE SECURITY OF THE INFORMATION COLLECTED

Finally, the Web site privacy policy should ensure consumers of a minimum level of security. A company provides security in the transmission of information by using encryption. Encryption scrambles and de-scrambles messages so that the unauthorized viewing of these messages is prohibited. However, the government is currently hindering the growth of encryption by insisting on the use of “key escrow, which allows the government to obtain the private key of any individual upon the showing of probable cause and with a court order.”141 Therefore, many industries are adopting new encryption standards, such as Secure Electronic Transaction (SET) and Pretty Good Privacy (PGP) protocols. Thus, the privacy policy should include a section discussing the type of

---

140 This “opt-in” method is consistent with a consumer voluntarily providing information to a company through the use of a registration form or other similar type of form. However, many companies prefer the “opt-out” method because this allows the company to gather information from the consumer indirectly through the use of cookies. The company collects this information without the consumer volunteering this information, and often without knowledge that the information is even being collected.

141 However, on September 28, 1999, the government recently released relaxed licensing requirements for the exporting of encryption. See Encryption Technology Export License Requirements Relaxed, (visited October 20, 1999) <http://www.foster.com>.
security used, as well as a brief explanation of its use.

VII. SAMPLE PRIVACY POLICY

The privacy policy below is based on the recommendations discussed in this Comment, as well as guidelines proposed by major participants in the electronic commerce field, such as BBB online. Some companies that maintain a Web site already adhere to these principles, but most do not. Thus, for the government-promoted industry self-regulation to work, all electronic commerce companies should adopt the following privacy policy.

WIDGET CORPORATION PRIVACY POLICY

Effective 1/1/2000

OUR COMMITMENT TO PRIVACY

The Widget Company believes that the establishment of trust and privacy is instrumental to the continued growth of the Internet. In order to inform you of the Widget Company’s policies and activities with respect to the collection and use of personal information on the Internet, the Widget Company provides this Internet Privacy Policy for review by users of its Web site.

DEFINITIONS:

“Personally identifying information” shall include, but is not limited to, first and last name, home or other physical address, email address, social security number, telephone number, or any information which when tied to the above items becomes identifiable to a specific individual.

“Disclosure” or “disclosed to third parties” shall mean (a) the release of information in personally identifiable form to another individual, firm or organization for any purpose or (b) making publicly available such information by any means including, but not limited to, public posting on or through home pages, pen pal services, email services, message boards or chat rooms.

“Archived database” shall mean Widget Company’s off-site “back-up” computer tapes containing member profile information.

“Child” or “Children” shall mean a person twelve (12) years of age or under.

INFORMATION WE COLLECT

This notice applies to all information collected or submitted on the Widget Company Web site. On some pages, you can order products, make requests, and register to receive materials. The types of personal information collected at these pages are: (1) Name, (2)
Address, (3) Email address, (4) Phone Number, (5) Credit Card Information.

In the course of using our site, the Widget Company may collect personal information through its Web site by using clicktrails and cookies. Cookies are small pieces of information that are stored by your browser on your computer’s hard drive. Among other reasons, cookies allow you to enter your password less frequently while on our Web site. All information collected by means of cookies or clicktrails will be anonymous, aggregated and used only by the Widget Company to track the traffic patterns and volume of use of its Web site. If you do not want to receive a cookie from this Web site, you may set your browser to refuse all cookies or to notify you when you receive a cookie, at which time you may then refuse the cookie.

If you send us personal correspondence, such as emails or letters, we may collect such information into a file specific to you. We use return email addresses to answer the email we receive. Such addresses are not used for any other purpose and are not shared with outside parties.

**OUR DISCLOSURE OF INFORMATION**

We do not sell, rent, or otherwise distribute any personally identifiable information about you to any third party. We do aggregate personally identifiable information and disclose such information in aggregate to advertisers and for other marketing and promotional purposes. However, in these situations, we do not disclose to these entities any information that could be used to personally identify you. Your credit card number, social security number and bank account number are not disclosed in aggregate at all.

We may also use personally identifiable information about you to deliver information to you that, in some cases, is targeted to your interests, such as targeted banners and promotions.

**OUR COMMITMENT TO DATA SECURITY**

The Widget Company has put in place certain technological and procedural security functions in order to protect the personal information it collects, uses or transfers from loss, misuse, alteration or destruction. Additionally, the Widget Company will use reasonable efforts to remove a user’s personal information from its archived database when it is no longer required for the purposes set forth above.

**OUR COMMITMENT TO CHILDREN’S PRIVACY**

Protecting the privacy of children is especially important. For that reason, we never collect or maintain information at our Web site from children we actually know are under age 13, and no part of our Web site is structured to attract anyone under 13 years of age.

**OPT-OUT POLICY**
Users of the Widget Company Web site are never required to provide any personal information in order to access or use its Web site. If at any point the Widget Company requests personal information, a user may opt-out of providing such information to the Widget Company, and the decision will not affect the user’s access to or use of the Widget Company Web site.

CORRECTING, UPDATING AND REMOVING PERSONAL INFORMATION

If a user’s personal information changes or is incorrect, please contact WCcorrections@email.com so that the Widget Company can maintain the accuracy and completeness of this information. In the event that a user of the Widget Company Web site decides to provide personal information and later wishes to have the Widget Company remove this personal information, please contact WCunsubscribe@email.com and the Widget Company will remove this information immediately.

To protect your privacy and security, we will also take reasonable steps to verify your identity before granting access or making corrections.

CONSUMER RECOURSE

Should you have other questions or concerns regarding your privacy while using the Widget Company Web site, please call us at (312) 555-1111 or send us an email at Widgetcompany@email.com

VIII. CONCLUSION

A privacy policy gives companies an opportunity to market their products throughout the Internet, while ensuring its customers that it will not collect and misuse their personal information. Until legislation provides consumers with trust in the network, companies must use self-regulation techniques to establish this trust. Establishing the trust of its customers is one of the most important aspects of a successful business today. By employing the privacy policy contained in this Comment, companies will be able to establish this trust, and gain an advantage over competitors who have failed to implement such a policy.