Loyola Consumer Law Review

Volume 9 | Issue 3 Article 13

1997

Regulating the Net: Case Studies in California and Georgia Show How *Not* to Do It

Barry Fraser
Staff Counsel & Dir. Of CyberCop Project-Utility Consumers' Action Network San Diego, CA

Regulating the Net: Case Studies in California and Georgia Show How *Not* to do it

by Barry Fraser

"The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks."[1] Originally developed in 1969 to link the military, defense contractors, and universities conducting defense-related research,[2] the Internet today has become a globally accessible medium connecting over 60,000 computer networks in over 90 countries.[3] Almost anyone with a personal computer, modem, and telephone line can connect to the Internet and "surf Cyberspace"[4] for information and interaction.

The growth of Internet usage has been phenomenal. In 1981, fewer than 300 computers were linked to the Internet. In 1989, this figure had grown to 90,000;[5] four years later, 1 million computers, were linked together. Now, estimates indicate that over 9.4 million computers are connected worldwide (60% of these computers alone are in the United States).[6] Furthermore, these astonishing figures do not include the millions of personal computers in homes, businesses, schools, etc. with access to the Internet via modem. Although it is very difficult to determine the precise number of current modem and traditional Internet users, approximately 40 million people around the world now use the Internet.[7] It is estimated that by the year 1999, 200 million people will use the Internet.[8]

The Internet's current popularity is fueled by its ability to provide a wealth of interactive communication services to the home. The Internet provides numerous beneficial services, such as electronic voting from home, the creation of electronic communities,[9] access to government officials,[10] access to vast amounts of information in physically remote locations,[11] access to electronic marketplaces where goods and services may be bought and sold,[12] and a multitude of interactive games and entertainment options.[13] The World Wide Web ("Web")[14] and other applications provide access to the Internet and allow consumers to access these services, view information, communicate with others, and make interactive purchases from their homes. The Web also allows users to download[15] text, graphics, photographs, and even audio and video clips to home computers.[16]

Barry Fraser is Staff Counsel and Director of the CyberCop Project (http://www.ucan.org) for the Utility Consumers' Action Network (UCAN), 1717 Kettnet Boulevard, San Diego, California, 92101, 619.696.6966. Mr. Fraser received his B.A. in Communications from the University of Memphis, his M.A. in Telecommunications from San Diego State University, and his J.D. from the University of San Diego. His E-mail address is bfraser@ucan.org.

The Internet is also attractive to businesses wishing to market goods and services:

> Electronic marketers instantly may access customers from Vermont to Vietnam. The interactive ad can become a 'virtual' store, where an advertiser completes the sale—and sometimes even the delivery of its products or services—online, blurring the lines [among] communication, distribution, and sales, and perhaps redefining advertising and marketing as we know them.[17]

Internet technologies enable marketers to track a consumer's behavior throughout a Web site[18] visit,[19] permitting them to identify new customers and better understand customer needs and desires.[20] The Internet is quickly becoming an important business tool. According to one estimate, advertisers spent $74 million on Internet advertising in 1996, and businesses spent $83 million in 1995 on developing Web sites.[21]

Many of the unique characteristics of the Internet which make it so appealing to merchants and consumers are also attracting malfeasants who perpetrate a variety of scams, frauds, schemes, and other consumer traps online. As "surfing the Net" gains popularity, the incidence of consumer abuses will undoubtedly increase. These risks will multiply dramatically as the Internet establishes itself as a commercial marketplace.[22]

Despite these warning signals, the Internet today is virtually unregulated. The Internet is neither stored within nor administered by any centralized agency.[23] Instead, the Internet operates upon the network of computers which constantly exchange and share communications.[24] Law enforcement officials and others voice concern that a lack of Internet regulation and consumer protection will breed widespread abuse that will curtail the Internet's exploding popularity and discourage audiences from full participation in its diverse content.[25]

On the other hand, concerned advocates have launched concentrated efforts on several fronts to prevent new legal restrictions on Internet activity. For example, organizations such as the Electronic Frontier Foundation ("EFF") (http://www.eff.org) and Computer Professionals for Social Responsibility ("CPSR") (http://www.cpsr.org/dox/home.html) engage in advocacy efforts to oppose Internet regulation on both the federal and state level. These advocates fear that regulation will dilute the unfettered, free-wheeling nature of the Internet, and, therefore, seek to keep this infant industry from being stifled by burdensome regulations. Many advocates cite First Amendment considerations as a justification for eschewing laws which attempt to limit new communication services. Furthermore, many argue that overly broad regulation will repress the rich diversity of content available online.[26]

"To regulate or not to regulate"—this is the question. This article serves two purposes. First, it provides a brief overview and description of the Internet and identifies the characteristics which make the Internet susceptible to consumer abuse. Second, the article explores the debate over Internet regulation by examining two relevant state laws enacted in 1996. In the California legislature, Assembly Bill 3320[27] requires a vendor conducting business on the Internet to make specified disclosures to a buyer, including: the vendor's return or refund policy, the vendor's legal name, and the street address where the business is operated. Under Georgia's Com-

puter System Protection Act,[28] it is a crime to use a name online that "falsely identifies" a speaker on the Internet. Additionally, it is a crime to publish information using trade names, logos or other symbols without authorization under Georgia's law.

Both the California and Georgia statutes contain serious defects which may be traced to the legislatures' unfamiliarity with the Internet and its applications. The Georgia law is overreaching and possibly unconstitutional while the law in California is confusing and ineffective. Neither of these statutes are acceptable as drafted. However, they provide examples to lawmakers in other jurisdictions of the mistakes which must be avoided in developing a regulatory strategy for reducing the risk of consumer abuse on the Internet.

I. An Introduction to the Internet

To communicate via this "network of networks" called the Internet, one must have access to a computer connected to a network. There are two common ways to link computers to a network. First, a computer or a computer terminal may be directly connected to a network that is itself connected to the Internet.[29] This method is most common in companies, educational institutions, government offices, public terminals at libraries, community facilities, and even some coffee shops. The second method of accessing the Internet, most common with home users, involves connecting a single personal computer to another computer or network of computers through a modem and telephone line.[30]

To access the Internet through a phone line, an individual generally must keep an account through an "Internet Service Provider" ("ISP") or a "commercial online service." An ISP will typically sell access to a telephone link attached to a larger computer, called a "server," which is connected to the Internet.[31] Commercial online services such as America Online, Microsoft Network, CompuServe, and Prodigy, provide access to their own proprietary networks which offer a variety of communication services and information available only to their subscribers.[32] In addition to offering access to these proprietary services, most of the popular commercial services now provide access to the Internet.

After establishing a connection to the Internet, one may communicate or retrieve information from any of the millions of publicly accessible[33] computers linked to the Internet. Communication and information exchange tools are available through the Internet, and these applications, while constantly changing, may be roughly grouped into five categories:[34]

(1) One-to-one messaging, such as E-mail. E-mail allows a user to send a message to any other user (or group of users) who is accessible through the Internet. Every individual opening an Internet account is assigned a unique address in a standard format (for example, bfraser@ucan.org) which enables mail properly addressed to reach the intended recipient.

(2) Electronic mailing lists, such as "listserv." Listservs allow many users to receive a single message concurrently. Electronic mailing lists operate by an individual submitting a message to the listserv manager, who then forwards it to other members on the list. Most electronic lists are topical, allowing members to keep abreast of developments in a particular subject area.

(3) Real time communication, such as Internet

Relay Chat ("IRC"). IRC and related chat forums allow an individual to send messages in "real time"[35] (e.g., instantaneous communication) so that remote recipients may read the text on their computer screens as the message is being typed. Chat groups are often topic-driven and are extremely popular. Thousands of individual chat groups may be in progress at any one time, with tens of thousands of users collectively engaging in these online "conversations."

(4) Distributed message databases, such as USENET newsgroups. Newsgroups are topical collections of messages which may be accessed in two different ways. First, an individual may "subscribe" to the newsgroup and be sent every message posted to that group via E-mail. Second, newsgroup messages are kept in a database, and a user may search for messages with specific topics, known as "threads." Newsgroups currently exist on more than 15,000 different subjects, with up to 70,000 individual messages posted to these groups each day.

(5) Remote information search and retrieval, such as "ftp," "gopher" and the "World Wide Web." Perhaps the most popular activity on the Internet is "browsing" or searching for information located on remote computers. There are three primary ways to access information on the Internet. The first is known as file transfer protocol or "ftp," which generates a simple list of computer files available on a computer and allows the user to pick one or more files to download. The second way to access information is by "gopher."[36] Gopher allows the user to view simple text files before downloading them. The third and by far the most popular information retrieval method today is the World Wide Web ("Web").

The Web combines a "graphical interface" which allows the user to view both text and graphics with a "hypertext" formatting language which allows the user to navigate from file to file by simply clicking on the specified text or graphics. These files are called "Web sites" or "home pages." Individuals and organizations may create and publish "home pages" which are graphically presented documents formatted in hypertext language linked to other related documents. These links may lead to documents on the same computer as the home page or documents located on other computers in remote locations. Web sites may also contain interactive forms which allow users to provide information to the Web site publisher. These forms may be used to join an organization, send E-mail, or purchase a product.

Individuals generally use one or more of these methods to conduct a myriad of activities on the Internet such as communicating with one or many other individuals; searching for news, sports, financial, or other specialized information; conducting transactions such as shopping, banking, and filling out forms and applications; and participating in entertainment activities including games, contests, and viewing audio and video clips of movies and music. The variety of subject matter and the ease in which can be accessed have made the Internet an incredibly popular and useful communication device for millions of people.

II. Consumer Traps on the Internet

The Internet provides many new and exciting methods for consumers to communicate and ac-

cess information, products and services. However, these new technologies also open the door to a host of potential consumer problems. One commentator divides these harms into the following categories:

(1) Computer Crimes–hacking (unauthorized access to computer systems), worms and viruses (computer programs which shut down the system or destroy information), and theft of data;

(2) Fraud–theft of credit or financial data, investment scams, pyramid marketing schemes, Ponzi schemes,[37] and deceptive advertising practices;

(3) Non-computer Crimes–distribution of child pornography or bomb manufacturing instructions, stalking, hate speech, and virtual gambling casinos.[38]

Abuse in all of these categories has increased in correlation with the rise of Internet use since 1989. For instance, the number of "hackings" or unauthorized accesses to computer systems has nearly doubled in each year since 1989.[39] State securities regulators in Missouri, New Jersey, and Texas alone began investigating over two dozen online financial and investment scams in 1994.[40] More recently, the Federal Trade Commission ("FTC") and state attorneys general have started to respond to increasing numbers of claims of false and deceptive advertising on the Internet.[41] Using its regulatory powers under various unfair competition and deceptive advertising regulations,[42] the FTC has prosecuted over a dozen cases involving online scams and false advertising.[43] In December 1995, the FTC teamed up with other federal, state, and local agencies to review Internet sites suspected of supporting illegal pyramid schemes.[44] Designated as "Internet Pyramid Surf Day," the review notified 500 Web sites that they may be promoting illegal activities.[45]

Using its regulatory powers under various unfair competition and deceptive advertising regulations, the FTC has prosecuted over a dozen cases involving online scams and false advertising.

Other evidence indicates that consumer abuse is a growing problem on the Internet. In July 1996, the Utility Consumers' Action Network ("UCAN") established the "CyberCop Complaint Center," a Web site where visitors may lodge complaints and inquire about consumer problems on the Internet.[46] In its first six months of operation, the site received hundreds of complaints and inquiries concerning a wide range of issues. Preliminary results indicate that the majority of complaints involved fraud and deceptive advertising practices, disputes with online service providers, and unsolicited or "junk" E-mail advertisements. Additional complaints involved issues such as misuse of private information, online harassment, and the availability of obscene and indecent materials to minors on the Internet. Other private organizations, including the Better Business

Bureau[47] and the National Fraud Information Center,[48] have established similar Web sites to monitor activity and provide information to Internet consumers.

III. Unique Characteristics of the Internet

Although many of the Internet abuses are simply online replications of more traditional telephone and mail scams, other abuses have taken advantage of the Internet's unique nature by creating new types of consumer harms. Four characteristics of the Internet tend to make online consumer abuse distinct, and perhaps more difficult to combat than the abuse associated with other communication media. These four characteristics are: (1) accessibility, (2) anonymity, (3) transience, and (4) interactivity. Although these features are the elements of the Internet that users enjoy, they are also the basis of the concern regarding online consumer abuse. Each characteristic is described in detail below.

Accessibility. The Internet has been called a "cheap speech" medium by one commentator because it is so easily accessible by both information consumers and providers.[49] Almost anyone with a telephone line, computer, and a modem can obtain an E-mail address and access to the Web. An E-mail account is usually included with a user's Internet or commercial service account, allowing a user to send and receive an unlimited number of E-mail messages at no additional cost beyond the provider account fee. In addition, software programs which allow users to send the same message to thousands of individuals simply by typing a few strokes on the computer keyboard are readily available.[50] The low cost of sending and receiving E-mail messages makes this technology very attractive to marketers desiring to provide sales and marketing materials to a large number of potential customers.

Likewise, virtually anyone may create a Web page and place content on the Internet for a very low cost, usually between $30-$50 per month.[51] Some Internet Service Providers supply free Web sites as an incentive to purchase an account with the service. Thus, it has become very easy and inexpensive to set up a site that is accessible to millions of Internet users. The ability of almost anyone to become an information producer is one of the primary attractions to the Internet and the Web:

> [W]hat's really exciting about the Web is that it's a two-way medium. With the World Wide Web, ordinary people can become information providers as well as information consumers. All kinds of people—slick mail order businesses, giant computer firms, college students, non-profit organizations, hobbyists, writers, poets, artists, and more—are creating their own Web documents and making them available for access.[52]

Minimal barriers for both speakers and listeners on the Internet provide easy access to all who wish to speak in the medium and create a relative parity among speakers (i.e., chat rooms), a parity which is not available in other electronic mass media.[53] This accessibility has been cited as the reason for the "astoundingly diverse content" found on the Internet.[54] Unfortunately, this accessibility makes it easier for fraud, e.g., "scam artists" to use the Internet to defraud, deceive, or

otherwise harm consumers.

Anonymity. It is relatively simple for Internet users to communicate or make information available anonymously or under an alias identity or "handle."[55] E-mail addresses often provide little or no indication as to the user's identity. Most Internet access providers neither require a detailed registration process nor request positive identification prior to setting up an account. Similarly, Web sites typically contain little if any indication or reference to the true identity of the individual or organization responsible for the site or even the physical location of the owner.

Some Internet newsgroups and chat groups encourage users to select an alias or "handle" by which an individual user is identified to the other users of the service. Other users cannot determine the true identity of an anonymous user unless the anonymous user chooses to reveal his or her identity. Additionally, Internet users may hide their true identities and even their true E-mail addresses by using "anonymous remailers," services which delete the real address of Internet transmissions and replace it with the address of the remailer organization. These services make it virtually impossible to trace messages back to the original sender.

The ability to remain anonymous on the Internet possess advantages and disadvantages. Anonymity allows an individual to speak about a subject without fear of being associated with the subject. In fact, the Supreme Court, in *McIntyre v. Ohio Elections Commission*[56] recognized a speaker's right not to reveal her identity in connection with political speech (or most likely literary, artistic and other speech). At least one commentator has argued that this protection should be extended to Internet activities.[57] Anonymity allows an individual to express an unpopular opinion or access sensitive information which may be embarrassing or harmful if the individual were connected with that information.[58] Additionally, anonymity can allow online users to prevent the collection of personal information concerning their viewing and shopping preferences, which can be easily collected on the Internet and used for marketing purposes.[59] Thus, anonymity is an essential element for some Internet users, and as with accessibility, enhances the diversity of content available.

Nevertheless, anonymity allows users to hide their real identities or impersonate someone else in order to harm other users. One author notes:

> Disguising the sources of messages or postings relieves their authors from responsibility for any harm that may ensue. This often encourages outrageous behavior without any opportunity for recourse to the law for redress of grievances. Law enforcement officials or lawyers seeking to file a civil suit might not be able to identify an individual to hold responsible.[60]

Anonymous speech is especially problematic to consumers because it both encourages the distribution of material which may be harmful and prevents consumers who are harmed from locating the perpetrators and holding them accountable.

Transience. The third important characteristic of the Internet is that it is constantly changing—"[i]t is a book forever being written, rewritten, revised and erased; it is a world that is inside one dimension of text on a screen, and yet

does not exist in physical space."[61] One court has proclaimed, "the strength of the Internet is chaos . . . ."[62] The Internet's transient quality creates not only an ever-changing parade of new and exciting ideas but also causes difficulty in locating the same information or resource more than once.

Web sites, for instance, do not remain static, but are constantly in a state of flux. New information is added and old information is deleted on a daily, or even hourly basis. Since users navigate from site to site through the use of hidden hypertext "links" which often "point" or connect the user to files buried in the hierarchy of a Web site, users may not always know where they are or how to later return to the site. Users often link to materials on Web sites which differ from the site they have chosen to visit without realizing that they have been connected to a different site.[63] Furthermore, retracing one's own path back to a specific site or document is sometimes impossible because one or more of the links pointing to the information may have been changed or removed.

E-mail accounts and Web sites are easy to establish, thus, they are also easy to shut down or move to a different service provider. Unfortunately, the E-mail and Web site addresses may change whenever such a move occurs, and a "mail forwarding" procedure is generally not available on the Internet. Furthermore, a user can register multiple E-mail and Web site addresses and simultaneously conduct business under several different "personas." Duplicating various locations makes it possible for scam artists to shift online locations quickly and easily. In sum, the transient nature of the Internet creates a dynamic and exciting experience for users and makes it easier for wrongdoers to cover their tracks and avoid precise detection in Cyberspace.

Interactivity. The most distinguishing characteristic of the Internet is its interactive nature. E-mail, newsgroups, and chat groups allow individuals to exchange comments in real time and to make these comments immediately available to others for review and response. Also, Web sites now incorporate elaborate forms and surveys, allowing visitors to disclose a wealth of information with only a few keystrokes. Software is now available which provides low cost interaction by live audio and even video-conferencing techniques.

The interactive qualities of the Internet have led many to believe that it will be ideally suited for electronic commerce by making it easy for consumers to buy and sell a wide array of goods and services online. While the ability to engage in electronic transactions might be convenient and time-saving for consumers, associated consumer risks (i.e., fraud) have reduced and limited large-scale commercial activity involving tangible goods (i.e., product ordering and direct marketing) on the Internet. The primary obstruction to electronic commerce has been the lack of secure methods of providing payment over the Internet. Until very recently, providing credit card numbers and the like over the Internet has been discouraged because of the risk that these numbers may be captured and stolen while in transit. However, recent advances in cryptography and other security techniques promise to reduce this risk considerably. In fact, most Internet and commercial online services now require the subscriber to provide a credit card number online in order to establish service. However, it remains to be seen whether the Internet will become a viable mass marketplace for tangible goods.

More promising is the potential of this medium for transferring intellectual property rights, such as written works, audio and video works, and computer software and games, which consumers may download. Additionally, "shareware" enables consumers to download computer software or files at no cost for an evaluation period, and pay later if satisfied with the product. Often, vendors will provide additional services, such as access to technical support or upgrades as an incentive for consumers to actually pay.

This interactivity is undoubtedly one of the greatest attractions of the Internet giving the consumer control and convenience and allows consumers to retrieve information, post an opinion, purchase a product, or conduct a transaction immediately. However, this characteristic makes it very easy to disclose financial, credit or other personal information to unknown or anonymous parties. According to one report:

> Entire transactions, from offer and acceptance to and perhaps delivery, can be accomplished with just a few clicks . . . . Once a secure online payment is in place, the sheer volume of transactions will present a real challenge to law enforcement. Electronic payment systems could reduce or eliminate delays or cooling off periods available to consumers under conventional payment systems such as personal checks and credit cards.[64]

In the words of another observer, "[u]nfortunately, the instantaneous nature of Internet advertising and transactions have created a fertile field for fraud."[65]

While the qualities of accessibility, anonymity, transience, and interactivity combine to create an exciting and diverse experience for Internet users, these elements also combine to breed a host of new and dangerous consumer traps for the unwary. As the Internet becomes more widely accepted, new participants will tend to be less informed and educated on how the technology works and the steps that must be taken to reduce the risk of online abuse. Correspondingly, the Internet will also attract greater numbers of malfeasants who wish to take advantage of the insulations from both detection and liability that the Internet provides. Thus, the scope and frequency of online consumer abuse will most likely continue to multiply as usage increases. These factors have resulted in calls for Internet regulation on the state level from legislators, attorneys general and law enforcement agencies.

IV. "To Regulate or Not to Regulate?"

The knee-jerk response to combating consumer abuse on the Internet has been to create laws which restrict or prohibit the characteristics which appear at first blush to be the cause of the problem. This is the wrong approach in developing a regulatory framework for the Internet. Rather, the four characteristics—accessibility, anonymity, transience, and interactivity—are the essence of the Internet and are what sets the Internet apart from other electronic media such as radio, television, and cable television. These characteristics are the main attraction of the Internet to consumers and the primary reason that the medium is enjoying such rapid growth.

Placing limits on these characteristics may actually limit the potential of the Internet.[66] Many users enjoy the sense of "anarchy" created by

the dynamic and unregulated nature of this medium and fear that all or part of the Internet may be "shut down or censored in the name of law and order."[67] Commercial developers of the Internet echo these sentiments and worry that the economic costs of compliance with inappropriate or overly broad regulation will raise barriers to entry and consequently diminish the Internet's commercial potential.[68]

Proponents of this rather arcane view often cite the First Amendment as the legal basis for keeping the Internet free of unnecessary regulation. In *ACLU v. Reno*, the court held that the Communications Decency Act ("CDA"), a portion of the federal Telecommunications Act of 1996 which would have prohibited indecent materials on the Internet, was unconstitutional under the First Amendment.[69] Relying on Justice Holmes' "marketplace of ideas" theory of the First Amendment,[70] the court found that the Internet "has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen."[71] The court noted the potential chilling effect of content regulation:

> As some speakers leave or refuse to enter the medium and others bowdlerize their speech or erect barriers that the Act envisions, and still others remove bulletin boards, Web sites, and newsgroups, adults will face a shrinking ability to participate in the medium. Since much of the communication on the Internet is participatory, *i.e.*, is a form of dialogue, a decrease in the number of speakers, speech fora, and permissible topics will diminish the worldwide dialogue that is the strength and signal achievement of the medium.[72]

Likewise, Internet consumer protection laws, particularly those directly regulating content, may cause a similar chilling effect.[73]

Lawmakers who wish to regulate the Internet are faced with a dilemma—how to protect consumers from recognized abuses that arise out of the Internet's unique characteristics (i.e., providing vast sums of information quickly). The immediate production of material is one of several reasons for the popularity of the Internet. Thus, the level of use increases daily. Three possible approaches may be taken: (1) eschew regulation and allow market forces to "self-regulate" the industry; (2) extend the scope of existing laws which currently apply to traditional consumer abuses; or (3) enact new laws and regulations aimed specifically at the nature of the abuse.

The free market, "self-regulation" approach has many supporters and is essentially the framework in most jurisdictions today. The best example of this approach is the treatment of unsolicited direct mail advertising (also known as "junk" mail) delivered by traditional postal services.[74] Direct mail advertising is, for the most part, unregulated.[75] A consumer who wishes to eliminate such mail must contact the responsible company and ask to be taken off of its mailing list. Unsolicited advertising messages are often time-consuming and obtrusive, but generally cause no great consumer harm.

However, Internet E-mail is much different from traditional postal mail and may harm consumers. As discussed earlier, it is very easy to search the vast numbers of newsgroups and collect names and E-mail addresses to form large electronic mailing lists. Unscrupulous market-

ers may use anonymous E-mail addresses, making it virtually impossible for the consumer to contact the marketer and ask to be removed from the list. These messages may then be personalized to appear as if sent from friends or acquaintances on the Internet, who "suggest" that a recipient visit a Web site or try a product. Web pages may be even more deceptive, disguising a sales pitch as an interactive game, contest, or even as "consumer information."

Compounding this problem is the adolescence of the Internet. Except for the most computer-savvy participants, users may not fully comprehend the technology well enough to protect themselves or their personal information. Consumers may be unfamiliar with the aspects of the technology which encourage anonymity and subtle deceptions, and the ease and speed of conducting an entire transaction with only a few keystrokes may lull consumers into unwanted actions. Also, the complexity of navigating the Internet may make it difficult for consumers to relocate the site or the service which deceived them. Thus, the potential for consumer harm may be much greater on the Internet than in other unregulated areas, such as direct mail.

Both law enforcement agencies and legitimate businesses have voiced concerns that unregulated activity may adversely affect the Internet:

> The commercial health of cyberspace will turn on consumer confidence. Doubts and insecurities could keep people away, capping the growth of the medium. Lawlessness, or even the threat of lawlessness, could dramatically limit the usefulness of the Internet to consumers.

Businesses, too, want consumers to feel "safe" while doing business in cyberspace and are rooting for this electronic medium to realize its potential. It would be a disaster for advertising in the cyberworld to lose credibility because of the ease of disseminating false claims.[76]

Supporters of Internet legislation have also argued that "[i]f abuses go unchecked, people will shy away from the Internet which, in the end, defeats the purpose and strength of this electronic, global communications network."[77] Therefore, if the Internet is to become a true mass communication medium comparable to television and radio, it is likely that some regulatory response will be necessary to make cyberspace a safer place for consumers.

The second regulatory approach—expanding the scope of existing consumer laws to include the Internet—has some appeal and may be successful on a limited basis. Many existing laws and regulations already apply to conduct on the Internet. For example, existing laws prohibiting deceptive advertising have been applied to Internet advertising.[78] However, many of these laws fail to provide adequate protection for Internet consumers because they were drafted long before the Internet existed as a consumer tool. Thus, these laws do not contemplate the unique characteristics of the Internet and will ultimately fail to provide adequate protection against the unique Internet problems which will arise.

Some lawmakers have attempted to fill these regulatory gaps by simply adding the words "and the Internet" to the laundry list of practices expressly prohibited by existing statutes.[79] However, the Internet contains new technologies such as E-mail that could not have been contemplated by the original drafters of the existing laws. Con-

sequently, adding "and the Internet" to these old laws is a patchwork remedy at best and may provide no additional help to consumers.

Furthermore, patchwork legislation can create paradoxical and contradictory language that may confuse judges and ultimately slow the judicial process. For example, the Electronic Communications Privacy Act ("ECPA")[80] of 1986 amended federal wiretap law to include electronic E-mail and other transmissions by adding the phrase "electronic communications" (and other language changes) to existing provisions.[81] Courts have expressed difficulty with this approach, stating that the complex law has become "famous (if not infamous) for its lack of clarity."[82] For instance, in *Steve Jackson Games v. United States Secret Service*,[83] the fifth circuit spent considerable time trying to determine whether the seizure of a computer containing E-mail sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an "intercept" proscribed by the ECPA.[84] Resolving this issue was challenging because E-mail transmission is technologically different from the transmission of telephone conversations, yet the definition of "intercept" in the statute did not take those differences into consideration. The court was forced to treat them similarly under the ECPA, and to hold that such a seizure was not an "intercept" under the statute, and thus was not protected.

The *Steve Jackson Games* case illustrates that simply adding a new technology to the protection granted by an existing law may be ineffective unless the entire law is revised to conform to the unique characteristics of the new technology. If lawmakers choose this approach, they should perform a comprehensive evaluation of the technology and do considerable research into the precise nature of the ensuing harms to ensure that all of the terms and provisions of the existing law conform to the unique aspects of the new technology. For new and uncharted technologies such as the Internet, however, it may be preferable to develop an entirely new regulatory regime rather than twist and contort existing law into conformity. New legislation addressing the Internet must be carefully contemplated and narrowly tailored to protect against only the specific harms at issue. Otherwise, the detrimental effects of such legislation may create more harm than originally intended to eliminate.[85] In sum, much care and planning must go into both the revising of current laws and the drafting of new Internet laws.

Unfortunately, efforts thus far to develop a workable regulatory approach to consumer protection on the Internet have fallen far short of the mark. The remainder of this article will examine two Internet consumer laws enacted in 1996: one in Georgia and one in California. While both laws contain elements which might be incorporated into useful state legislation, neither the Georgia nor the California law is currently useful to consumers, and both contain provisions which will likely lead to more harm than good regarding the new medium.

V. Georgia's Approach: The Computer Systems Protection Act

The state of Georgia enacted legislation which attempts to address the issue of consumer fraud on the Internet. Georgia House Bill 1680, officially titled The Georgia Computer Systems Protection Act ("the Georgia Act"),[86] is aimed at "computer related crime" which the legislature determined to be a "growing problem in the gov-

ernment and in the private sector."[87] While the majority of the Act's provisions address crimes such as the unauthorized use of computer facilities or the theft, alteration or destruction of computer records, one section of the Georgia Act makes it unlawful to "knowingly" transmit misleading data over a computer or telephone network for the purpose of "setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information."[88]

"Misleading data" is defined by the Georgia Act in two ways: (1) data which uses "any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data" or (2) data that "implies that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained."[89] A violation of these provisions constitutes a misdemeanor.[90] The Georgia Act expressly exempts telecommunications companies and Internet access providers who merely transmit misleading data for their customers. Additionally, the Georgia Act includes a very broad venue provision which allows an action to be brought in "any county in which, from which, or through which, any use of any use of a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication."[91]

The Georgia Act places broad restrictions on Internet activity in two ways. First, it appears to criminalize the use of "individual names" that "falsely identify" the user in an E-mail account or Web page.[92] Thus, the Georgia Act strikes right at the heart of anonymity on the Internet, making the use of any name other than one's real name a potential violation of the law. Second, the statute's restriction of unauthorized use of trademarks may prohibit the creation of Web site links to a trademarked site without permission.[93] The linking of sites is an inherent characteristic of the Internet. This law restricts both the accessibility and the transient qualities of the Internet by limiting users' ability to freely navigate between Web sites.

[The] law restricts both the accessibility and the transient qualities of the Internet by limiting users' ability to freely navigate between Web sites.

The statute is currently under attack in federal court, as unconstitutional under the First Amendment and Commerce Clause of the United States Constitution.[94] In addition to the potential Constitutional problems on the federal level, the Georgia Act contains four additional problems. First, the requirement of malicious intent is conspicuously absent. The Georgia Attorney General claims that the Georgia Act only applies to the fraudulent practice of misrepresenting someone else's identity or trademark and not anonymous communications or the use of pseud-

onyms.[95] However, the Georgia Act contains no specific intent language, other than mere "knowledge" of the transmission itself. One commentator notes the danger of this omission:

> Because fraud and malicious intent are not elements of the statute, a prosecutor conceivably could interpret any name other than the user's actual name to be "false." Furthermore, it may be possible to convince a Net-naive judge that anonymity on the Internet is bad public policy and, as such, should be proscribed by the statute.[96]

Second, the Georgia Act attempts to forbid all anonymous activity, not just harmful anonymous activity. As explained above, anonymity is desirable and even essential for some Internet users in certain situations. As the *McIntyre v. Ohio Elections Commission* court held, at least some types of anonymous speech deserve First Amendment protection. [97] While this broad prohibition would certainly reduce the risk of many types of consumer abuse on the Internet, it will also severely inhibit speech and diminish the vitality of the Internet.

Third, the Georgia Act is vague and ambiguous. It is unclear whether a simple E-mail alias is an "individual name" under the statute, and the term "falsely identifies" is not defined. Moreover, the language pertaining to unauthorized use of trademarks is unclear and fails to specify what specific types of activity are prohibited. In fact, the law as written is likely unconstitutional on its face because of its extraordinary breadth and vagueness.[98] It will be difficult for Internet users, law enforcement officials, and courts to determine precisely how to comply with or enforce the statute. The law is by no means narrowly tailored to a necessary purpose, and a variety of less restrictive means are available to address the same harms.

Finally, the Act's limitation on linking to trademarked sites not only restricts the essential Internet qualities of accessibility and transience but also displays a glaring lack of understanding by the legislators about how the Internet operates. Virtually all commercial Web sites strive to increase the number of visitors to the site. The creation of links to the site simply provides another "path" for visitors to reach the site. Common sense dictates that the owner of a trademark would wish to encourage links to the site, rather than discourage access by the threat of criminal sanctions. This stark misunderstanding of the working of the Internet prompted one Georgia lawmaker to assert that the law was passed by "legislators who don't know a gigabyte from a chigger bite."[99]

The Georgia Act demonstrates the problems encountered in applying sweeping prohibitions to the Internet. Although the Georgia Act does succeed in identifying anonymity, accessibility, and transience as the basis for many consumer harms, it tries to deter these harms by prohibiting activities that are essential to the character of the medium. This approach displays an acute lack of understanding of the Internet on the part of the drafters and suggests a minimal investment of forethought or planning in the drafting of the law. The result is a failure to properly balance the important issues of free speech, intellectual property rights, and criminal intent. Finally, the Georgia Act is vague and ambiguous, and many of the important terms are not properly defined. The end-product is a law that will be difficult to apply to the wide diversity of situ-

ations likely to arise on the Internet and will afford little consumer protection.

VI. California's "Gentle" Approach to Internet Regulation

California legislators took a different approach in enacting Assembly Bill 3320 ("the California Act").[100] According to the bill's sponsors, the California Act applies a "gentle approach,"[101] by placing some "basic, minimum protections" for consumers who wish to "shop electronically" on the Internet.[102] The California Act amends California Business and Professions Code section 17538 by adding the words, "Internet or other electronic means of communication" to existing provisions regulating mail-order sales.[103]

There are two relevant parts to the California Act. First, the California Act makes it unlawful for anyone selling or leasing goods or services to accept payment from a buyer for the purchase or lease of goods or services ordered by "Internet, or other electronic means of communication," unless the seller complies with certain statutory requirements applicable to mail order, telephone, and catalog sales within 30 days from the sale or lease.[104] The vendor must either provide the ordered goods, refund any prepayments, or provide substitute goods and offer the buyer the opportunity to reject them. This broad provision applies to anyone who: (1) leases goods or services over the Internet, (2) offers for sale goods or services that may be ordered over the Internet, or (3) includes an Internet address in advertising promoting such sales or leases.[105] However, the goods or services must actually be ordered over the Internet for the requirements to apply.

Second, the California Act requires an Internet vendor to provide an E-mail, written, or on-screen notice of the vendor's return and refund policy and the legal name and address of the business before accepting payment.[106] If the disclosure is made by on-screen notice, a vendor must comply with the following provisions:

(1) The information must appear on either the first screen displayed when the vendor's site is accessed, the screen on which the goods are first offered, the screen on which the buyer places the order, or the screen on which the buyer enters payment information;

(2) the type face of the disclosure must be no smaller or less legible than that offering the goods or services;

(3) the disclosure must be accompanied by an adjacent statement describing how the buyer may receive the information at the buyer's E-mail address, and must be provided within five days if the buyer so requests; and

(4) the vendor may provide a private mailbox number in lieu of a street address, so long as the private mailbox provider is in compliance with California law regarding receipt of service at private mailbox addresses;[107]

The disclosure notice must be provided for any transaction which "involves a buyer located in California" even though the California Act is silent as to how the merchant is to determine whether a Web site visitor is actually located in that state.[108] This provision effectively requires all merchants operating a Web site anywhere in the world to comply with California law because any Web site might attract a visitor located in California. However, the California Act does not

address the method by which California law enforcement officials may reach such out-of-state defendants. Any violation of these provisions constitutes a misdemeanor punishable by imprisonment for up to six months and/or a fine of up to $1000.[109]

The California Act serves as a classic example of an attempt to stretch and bend existing rules to fit the new online environment. The existing California law was drafted to apply to specific harms which arise in the course of mail-order catalog transactions and which are caused by the substantial delay between *payment* for the goods and *delivery or receipt* of the product—a characteristic inherent to deliverable transactions. Generally, the buyer must prepay for the goods before shipment; therefore, the buyer bears the risk that the shipped goods will differ from those ordered, or that they will not be delivered within a reasonable period of time.

It is questionable whether the simple addition of the phrase, "Internet or other electronic means of communicating" provides any additional protection not accorded by existing law. Goods ordered via the Internet and then mailed to the consumer are clearly "mail order" goods and, therefore, already fall under the statute. Legitimate businesses moving from traditional mail order transactions to the Internet will already have such procedures for delays or substitutions in place. Fraudulent actors will likely not be deterred and will simply ignore the rules because they will be able to close up an anonymous site under investigation and simply open another site under a different alias.

Additionally, the language of the section which was crafted for mail-order transactions fails to address many other types of online transactions which will likely lead to significant consumer abuses. For instance, many online sales occur by instantaneous exchange of credit information where a buyer purchases a file to be downloaded. Other online vendors will provide shareware to the consumer, who will not be obligated to pay the purchase price until after an evaluation period. Still other sites will offer memberships which allow the consumer to browse the archives of the vendor and to pick and choose goods at the consumer's leisure. For example, a photographer might set up an Internet Web site to sell her photographs and allow buyers to download a digital file of the work immediately after the purchase. Likewise, an online legal service might sell access to archives of legal documents to lawyers, who may download the files immediately. These instantaneous transactions would therefore rarely present any risks of the nature addressed by the California Act.[110]

Other concerns not addressed by this law may be raised, however. For example, consumers may experience problems enforcing a warranty when a product purchased over the Internet is later found to be defective. This problem may be compounded when the defect arises a long time after the product is purchased, and the Internet site can no longer be found. Other types of consumer abuse, such as piracy of intellectual property or passing-off of counterfeit goods, may become prevalent on the Internet. For instance, a software program may be purchased and downloaded and only much later found to have been copied without authorization. Buyers may have remedies for these abuses under appropriate warranty or intellectual property law, but the California Act at issue here is unlikely to prove helpful to consumers.

The disclosure requirements of the California Act provides important information for consum-

ers who need to contact a reputable vendor to resolve a dispute regarding a transaction. Similar provisions should be encouraged in all states. However, in many cases, simply contacting the vendor may not resolve the consumer's problem. Unless the consumer can use the information to enforce other rights or remedies, merely providing a name and address may be of little value to the consumer. This is particularly true if the vendor is located in a jurisdiction far removed from the buyer.

Moreover, these disclosure requirements may provide little assistance to consumers who are dealing with a sophisticated Internet con artist. There is no quick and easy way to verify that the name and address disclosed is actually valid. Many consumers may potentially be deceived by online scams with seemingly legitimate business names and addresses only to find that the information is false or outdated and that the wrongdoer is unreachable. Thus, these disclosure requirements may do little to ensure that consumers can actually contact the vendor if a problem occurs.

Finally, the California Act includes a complex, technically narrow definition of "Internet" but leaves the term "other electronic means of communication" entirely undefined.[111] It is incomprehensible why the "Internet" should be defined so precisely and "other electronic means of communication" not defined at all. Commercial online services such as America Online or CompuServe which provide services very similar to those found on the Internet may not fall under the current definition. A court interpreting this law may place a narrow restriction on its scope and decline to extend it to services not specifically conforming to the definition as written. This conceivably would exclude a substantial number of online services which should be regulated under the statute. At the very least, the lack of precision will be the basis for much confusion and concern among Internet vendors attempting to comply with the statute.

All in all, the California statute, while taking a different approach from the Georgia statute, is defective for many of the same reasons. The drafters of the California legislation fail to demonstrate a thorough understanding of the nature of Internet communication and fall into the trap of forcing traditional laws to fit new modes of commerce. The California Act imposes a complex set of regulations on all online vendors rather than focusing on specific risks to consumers or specific practices. Furthermore, the California Act fails to include important definitions that would aid both compliance and enforcement. This "gentle approach," while perhaps less onerous than a broad sweeping regulatory agenda, creates rules that are ineffective, difficult to apply, and may be unnecessary for the majority of online transactions.

VI. Conclusion

While neither the Georgia nor California statutes are entirely devoid of merit, each contains significant defects that should cause legislators to question these types of approaches and attempt to solve the defects before adopting similar legislation in other jurisdictions. The following rules may serve as guidelines for planning a regulatory response to online consumer abuses.

First, new legislation restricting activity on the Internet must not target the specific characteristics of accessibility, anonymity, transience, and interactivity per se, but should instead focus on the application of these qualities for criminal or

harmful purposes. Accordingly, a specific criminal intent element should be included in any such legislation.

Second, statutes regulating activity on the Internet must be narrowly tailored to address specific conduct which is likely to harm consumers, while not prohibiting conduct which attracts consumers to the Internet. Definitions must be precise and crafted to fit the technology because common terms may take on new meanings when applied to the new medium.[112]

Third, a thorough understanding of the technology is an essential prerequisite to the drafting of any new rules for the Internet. Regulators should not fall into the trap of thinking that the Internet is simply traditional communication using computers. Rather, the Internet should be viewed as an entire new way of communicating.

Finally, regulators should not lose sight of the fact that the regulated activity is primarily speech and, thus, is subject to First Amendment protections. The nature of Internet communication has made the expression of a diversity of viewpoints and opinions possible. The new technological developments demand careful and thoughtful treatment when attempting to balance First Amendment protections against the need to confront harmful Internet activity. A failure to carefully consider the effects of new rules on protected speech will risk challenge on constitutional grounds.

The Internet is a unique technology that poses unique problems for consumer protection. The greatest threat to the development of this medium is that it will be forced into the same categories as other prior communication media. To avoid this outcome, regulators must spend considerable time developing an understanding of these new communication tools and their benefits and detriments prior to formulating any consumer protection strategy.•

ENDNOTES

[1] ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996). The Internet itself and the various applications used on the Internet are described in greater detail in the following section.

[2] *Id.* at 831.

[3] Consumer Protection Policy, 425 Trade Reg. Rep. (CCH) Federal Trade Commission Staff Report Volume II, 22 (June 12, 1996) [hereinafter *Consumer Protection Report*]. This Report is also available on the Internet (last visited Mar. 27, 1997) <http://www.ftc.gov/WWW/opp/global.htm>.

[4] The term, "Cyberspace" is a popular term which describes the entire experience of communicating via computer networks. William Gibson first used this term in his 1984 novel, Nueromancer. WILLIAM GIBSON, NUEROMANCER 51 (1984). *See, e.g.*, Anne Wells Branscomb, *Anonymity, Autonomy and Ac-*

countability: Challenges to the First Amendment in Cyberspaces, 104 YALE L.J. 1639, 1679 n.3 (1995).

The term, "surf" or "surfing the Net" is a popular term describing the activity of "browsing" or "searching" the Internet, sometimes in a random fashion, for information or content.

[5] *ACLU*, 929 F. Supp. at 831.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Similar to community action groups in the real world, electronic communities are groups of individuals with like interests who communicate via the Internet to create change or action.

[10] Branscomb, *supra* note 4, at 1639.

[11] Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER AND HIGH TECH. L.J. 403, 406-07 (1996). *See also Consumer Protection Report*, *supra* note 3 at 22.

[12] *Consumer Protection Report*, *supra* note 3, at 23.

[13] Adams, *supra* note 11, at 407.

[14] The World Wide Web ("Web") is a remote information retrieval application which may be accessed through the Internet. This process is described in more detail in the following section.

[15] The term "download" means to transfer a computer file from a remote location to local computer, such as a home PC.

[16] *Consumer Protection Report*, *supra* note 3, at 22-3.

[17] *Id.*

[18] A "Web site" is a set of information that a company, organization, educational institution, or individual provides on the Internet.

[19] This is normally done by asking a web site visitor to complete a registration form while online. Once a visitor has registered, every page that the visitor views in that Web site as well as everything purchased in that site is recorded. New technological advances may soon permit visitor tracking even if the visitor chooses not to register with the Web site.

[20] *Consumer Protection Report*, *supra* note 3, at 24.

[21] Richard Raysman & Peter Brown, *Regulating Internet Advertising*, 215 N.Y. L.J. 3 (1996).

[22] *See, e.g., Consumer Protection Report*, *supra* note 3, at 22-30.

[23] *ACLU*, 929 F. Supp. at 832.

[24] *Id.*

[25] *Id.* at 878.

[26] *See, e.g.*, Doug Willis, *Panel OKs Bill to Protect Consumers on Internet*, SAN DIEGO DAILY TRANSCRIPT, May 8, 1996, at 2A; California Alliance for Consumer Protection, *Consumer Traps on the Internet*, (visited Mar. 24, 1997) <http://consumers.com/fraudreport.html>.

[27] CAL. BUS. & PROF. CODE § 17538 (West 1996)

[28] Georgia's Computer System Protection Act, GA. CODE ANN. § § 16-9-90—93.1(a) (1996)

[29] *ACLU*, 929 F. Supp. at 832.

[30] *Id.*

[31] *Id.* at 833.

[32] *Id.*

[33] Many other computers and networks on the Internet are "private" and have restricted access only to subscribers or members, usually through a password procedure.

[34] Many recently published articles, and at least one court case provide comprehensive descriptions of the various Internet applications available today. *See generally*, *ACLU*, 929 F. Supp. at 834-37; William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 WAKE FOREST L. REV. 197, 200-03; Adams, *supra* note 11 at 406-08; BRYAN PFAFFENBERGER, WORLD WIDE WEB BIBLE 23-34 (1995). The following description of the Internet and its applications relies heavily on these sources.

[35] The term "Real time" refers to communication in which the message is sent and received instantaneously—for instance, in everyday, face-to-face chatting, or telephone conversations. Real time communication by means of computers usually occurs when the sender types a message with a computer keyboard that the receiver views instantaneously on a remote monitor.

[36] The name "gopher" comes from the University of Minnesota mascot, the Golden Gopher. The gopher software was developed at the University of Minnesota.

[37] A "Ponzi scheme" is a pyramid marketing scam in which money is paid out to initial investors first creating the illusion of legitimacy.

[38] Adams, *supra* note 11, at 409-16.

[39] *Id.* at 409-10.

[40] *See* Albert B. Crenshaw, *Con Artists Adapt Scams for Cyberspace Rip-Offs*, WASH. POST, July 3, 1994, at H1; Francis Flaherty, *Cyberspace Swindles; Old Scams, New Twists*, N.Y. TIMES, July 16, 1994, at 35.

[41] Robert W. Lehrburger, *Cyberpolice Crack Down on Deceptive On-Line Ads*, 215 N.Y. L.J. 1 (1996).

[42] 15 U.S.C.A. § 45 (West 1997) (prevention of unfair competition); 15 U.S.C.A. § 52 (West 1997) (false advertising); 16 C.F.R. § 435.1 (1997) (mail or telephone merchandise rule).

[43] Eleven of these cases resulted in consent judgments, which are set forth at 61 Fed. Reg. 14309-14332, and one action, FTC v. Brandzel, No. 96-C-1440 (N.D. Ill. filed March 14, 1996) reached a settlement in September, 1996. All cases involved a variety of online marketing schemes, including credit repair misrepresentations, fraudulent income opportunities, and computer equipment scams. *See*, Lehrburger, *supra* note 41, at 4.

[44] 452 Trade Reg. Rep. (CCH) (Dec. 17, 1996).

[45] *Id.*

[46] The author is director of the CyberCop Complaint Center, which

may be found on the Internet (last visited Mar. 26, 1997) <http://www.ucan.org>.

[47] Located (last visited Mar. 26, 1997) <http://www.bbbonline.org>.

[48] Located (last visited Mar. 26, 1997) <http://www.fraud.org>.

[49] Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 121 (1996).

[50] Many of the software programs used to communicate or retrieve information over the Internet are available as "freeware" or "shareware" and may be downloaded and used at no cost by anyone who has access to the Internet.

[51] *See, Consumer Protection Report, supra* note 3, at 4.

[52] BRYAN PFAFFENBERGER, THE WORLD WIDE WEB BIBLE, 2 (1995).

[53] *ACLU*, 929 F. Supp. at 872-73.

[54] *Id.*

[55] *See generally* Tien, *supra* note 49; Branscomb, *supra* note 4.

[56] 514 U.S. 334 (1995) (statute forbidding anonymous political pamphlets and other writings struck down as unconstitutional); *see* Tien, *supra* note 49, at 123.

[57] Tien, *supra* note 49, at 121.

[58] *See* Declaration of Shari Steel, ACLU v. Miller, 929 F. Supp. 824 (N.D. Ga. 1996) ¶¶ 40-43; (last visited March 26, 1997) <http://www.eff.org/pub/Legal/Cases/EFGA_v_GA/960924_eff.affidavit>. In some cases, anonymity is a necessary security measure. For instance, the personal safety of human rights dissidents, domestic abuse victims, and whistleblowers would be compromised if they could not communicate anonymously.

[59] *Id.* ¶ 44. For example, E-mail sent to topical newsgroups, mailing lists, and Web sites include the sender's name and E-mail address which are saved as part of the E-mail message. These names and E-mail addresses may then be collected and compiled into large marketing mailing lists. If techniques to preserve anonymity are used, the individual's true name and E-mail address will not be added to these lists.

[60] Branscomb, *supra* note 4, at 1642-43.

[61] Tien, *supra* note 49, at 184 (quoting Nancy Kaplan & Eva Farrell, *Weavers of Webs: A Portrait of Young Women on the Net*, THE ARACHNET ELECT. J. ON VIRTUAL CULTURE, vol. 2, no. 3, para. 37 (July 1994)).

[62] *ACLU*, 929 F. Supp. at 883.

[63] Stuart Levi, *Web-Site Hypertext Links Raise Issues of Control*, Nat'l L.J., Aug. 12, 1996, at B12.

[64] *Consumer Protection Report, supra* note 3, at 28-29 (footnotes omitted).

[65] Raysman & Brown, *supra* note 21, at 3.

[66] *See, e.g.*, Jeffery R. Kuester, *Cyber-Sheriff's in Town*, NAT'L L.J., July 1, 1996, at C1.

[67] Adams, *supra* note 11, at 416.

[68] *Id.* at 408; *see generally, ACLU*, 929 F. Supp. at 878.

[69] *ACLU*, 929 F. Supp. at 883; *see also* Adams, *supra* note 11 at 407.

[70] *ACLU*, 929 F. Supp. at 880 (citing Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. dissenting).

[71] *Id.* at 881.

[72] *Id.* at 879.

[73] *See e.g.*, Jerry Berman & Daniel J. Weitzner, *Abundance and User Control; Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619, 1634 (1995) (arguing that content regulation of any type of speech, including commercial speech, is inappropriate for interactive media, such as the Internet, because "user-control" technologies will become available to "filter out" objectionable materials).

[74] Because postal mail is much slower than Internet E-mail, it is often referred to in Cyberspace as "snail" mail.

[75] *See generally*, Privacy Rights Clearinghouse, *Junk Mail: How Did They All Get My Address* (last visited March 23, 1997) <http://www.privacyrights.org/fs/pub.html>.

[76] *Consumer Protection Report, supra* note 3, at 27 (footnotes omitted).

[77] California Senate Committee on Business and Professions, 1995-1996 Session, Legislative Council Analysis of Assembly Bill 3320, June 24, 1996. *See also, Consumer Traps on the Internet, supra*, note 26.

[78] FTC v. Corzine, No. S-94-1446 (E.D. Ca. 1994); FTC v. United States Telemedia, Inc., No. 96C-1440 (N.D. Ill. filed Mar. 13, 1996). *See*, Raysman & Brown, *supra* note 21, at 3.

[79] *See, e.g.*, 1996 Cal. Legis. Serv. Ch. 785 (A.B. 3320) (West).

[80] 18 U.S.C. § 2510 *et. seq.* (1996).

[81] *Id.*

[82] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994) (citing Forsyth v. Barr, 19 F.3d 1527, 1542-43 (5th Cir. 1994), *cert. denied*, 513 U.S. 871 (1994).

[83] *Id.*

[84] 18 U.S.C. § 2511(1)(a) (1996).

[85] The best example of the complication of "new" technology (e.g., Internet) regulation on the federal level was the Communications Decency Act ("CDA"), Title V of the Telecommunications Act of 1996, Pub. Law No. 104-104 § 502, 110 Stat. 56, 133-135. Enacted by Congress in an attempt to restrict "indecent" material on the Internet, the court struck down the law as unconstitutional under the First Amendment, in part because the CDA was not narrowly tailored and would diminish diversity of content on the Internet. *See, ACLU*, 929 F. Supp. at 855-56.

[86] GA. CODE ANN. § 16-9-90 (1996).

[87] GA. CODE ANN. § 16-9-91 (1996).

[88] GA. CODE ANN. § 16-9-93.1(a) (1996). Section (a) reads:

(a) It shall be unlawful for any person, any organization, or any representative of any organization knowingly to transmit any data through a computer network or over the transmission facilities or through the network facilities of a local telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted symbol for such purpose when such permission or authorization has not been obtained; provided, however, that no telecommunications company or Internet access provider shall violate this Code section solely as a result of carrying or transmitting such data for its customers.

[89] *Id.*

[90] GA. CODE ANN. § 16-9-93.1(b) (1996).

[91] GA. CODE ANN. § 16-9-94 (1996).

[92] Kuester, *supra* note 66.

[93] *Id.*

[94] ACLU v. Miller, 929 F. Supp. 824 (1996).

[95] Pamela Mendels, *Georgia Defends Its Internet Fraud Law*, N.Y. TIMES ONLINE, November 9, 1996 (last visited March 23, 1997) <http://www.nytimes.com/>.

[96] Kuester, *supra* note 66.

[97] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

[98] GA. CODE ANN. § 16-9-93.1(a) (1996).

[99] *Id.*

[100] CAL. BUS. & PROF. CODE § 17538(a) (West 1996).

[101] Rebecca Smith, *New Law Would Throw Net Over Computer Fraud*, SAN DIEGO UNION-TRIBUNE, ComputerLink, May 21, 1996, at 8.

[102] Floor Analysis, Assembly Bill 3320, California Senate Rules Committee (Aug. 7, 1996).

[103] CAL. BUS. & PROF. CODE § 17538(a) (West 1996).

[104] CAL. BUS. & PROF. CODE § 17538(a) reads in pertinent part:

It is unlawful in the sale or lease or offering for sale or lease of goods or services, for any person conducting sales or leases by telephone, Internet or other electronic means of communication, mail order, or catalog in this state . . . to accept payment from or for a buyer . . . and then permit 30 days, unless otherwise conspicuously stated in the offering or advertisement, or unless a shorter time is clearly communicated by the person conducting the sale or lease, to elapse without doing any one of the following things:

(1) Shipping, mailing, or providing the goods or services ordered.

(2) Mailing a full refund or, if payment was made by means of a transfer from an account, (A) crediting the account in the full amount of the debit, or (B) if a third party is the creditor, issuing a credit memorandum to the third party who shall promptly credit the account in the full amount of the debit.

(3) Sending the buyer a letter or other written notice (A) advising the buyer of the duration of an expected delay expressed as a specific number of days or weeks, or proposing the substitution of goods or services of equivalent or superior quality, and (B) offering to make a full refund, in accordance with paragraph (2), within one week if the buyer so requests. The vendor shall provide to the buyer in that letter or written notice a toll-free telephone number or other cost-free method to communicate the buyer's request for a full refund. If the vendor proposes to substitute goods or services, the vendor shall describe the substitute goods or services in detail, indicating fully how the substitute differs from the goods or services ordered.

(4) (A) Shipping, mailing, or providing substitute goods or services of equivalent or superior quality, if the buyer is extended the opportunity to return the substitute goods or services and the vendor promises to refund to the buyer (i) the cost of returning the substitute goods or services and (ii) any portion of the purchase price previously paid by the buyer....

[105] The law does not apply to transactions initiated by an "electronic agent" if the transaction does not exceed ten dollars. Cal. Bus. & Prof. Code § 17538(e)(5). "Electronic agent" is defined as a computer program designed to initiate or respond to electronic messages or performances without review by an individual. *Id.* at (e)(7).

[106] CAL. BUS. & PROF. CODE § 17538(d) (1996).

[107] CAL. BUS. & PROF. CODE § 17538(d)(2)-(3) (1996).

[108] CAL. BUS. & PROF. CODE § 17538(d) (1996).

[109] CAL. BUS. & PROF. CODE § 17538(f) (1996).

[110] It is unlikely that section 17538 of the California Business & Profession Code is even applicable to such transactions. The definition of goods limits the term to "tangible chattels" while most intellectual property rights are considered to be intangibles. This is unfortunate because the Internet is ideally suited to transactions involving intangibles such as literary works, digital audio and video works, and computer software licenses.

[111] The "Internet" is defined for purposes of the law as:

The global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions; and is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols; and provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

CAL. BUS. & PROF. CODE § 17538(e)(6) (1996).

[112] *See, ACLU*, 929 F. Supp. at 883.