Vanderbilt Journal of Entertainment & Technology Law

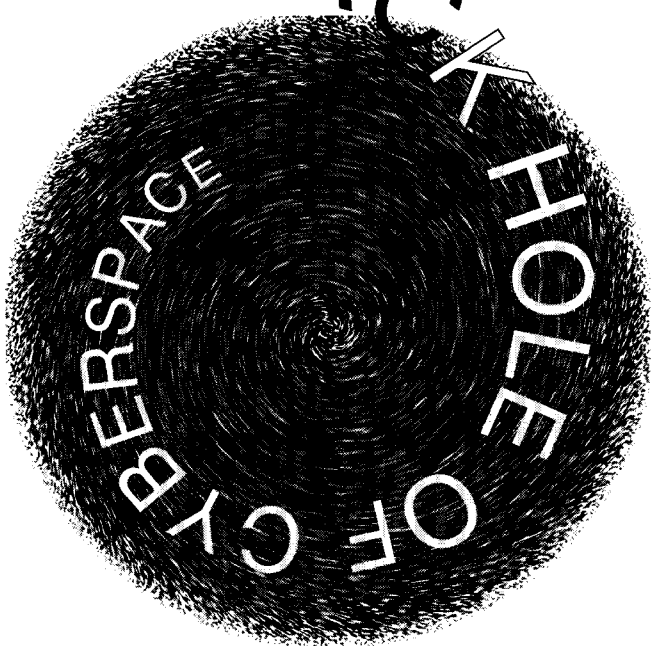
Volume 1 | Issue 1 Article 5

1999

Filling the Black Hole of Cyberspace: Legal Protections for Online Privacy

R. Craig Tolliver

FILLING THE BLACK HOLE OF CYBERSPACE



"The Internet is 'a unique and wholly new medium of worldwide human communication.'"[1] This pronouncement of the United States Supreme Court echoes what most of the American population has known for some time. The emergence of cyberspace has dramatically changed the nature of electronic communications, and consumers are conducting online transactions at a tremendous pace.

While this revolution has obviously increased the amount and types of information available to American consumers, it has also achieved a different result: businesses now have access to an unprecedented amount of personal information. In turn, there exists a danger that this information will be used by the businesses in a way that abuses the consumer. This Note will address the current state of the law regarding privacy of consumers' personal information, its inadequacies, and the reasons why the United States should adopt a statutory framework to regulate the use of personal information collected by businesses.

LEGAL PROTECTION FOR ONLINE PRIVACY

BY R. CRAIG TOLLIVER

NATURE OF THE PROBLEM

Imagine that you are "surfing the Internet" one day when you come upon a webpage that claims to have established a large database of information on Internet users. Even though this database operator will eventually charge a fee for its use, it is currently offering users a free search of the database. Imagine further that the database claims to have grouped information by the e-mail addresses of users, even though it promises to eventually assign "real" legal names to each of these e-mail addresses. After typing in your own e-mail address and running a search, you are shocked to learn that the database has a listing of your "most visited" Internet sites, along with other private information such as a compilation of many of your online purchases and catalogue orders. After you contact your attorney, you are even more shocked to learn that this type of online snooping and information gathering is legal. Indeed, on the Internet it seems that nearly everything is fair game.

The Internet is a highly decentralized, global network which is unique among communications media in the variety and depth of personal information generated by its use. When users browse the World Wide Web, they leave a series of electronic markers, or "clickstream," on each site that they visit. A website can capture certain information about users as they enter that site. This information includes the user's e-mail address, the type of browser used, the type of computer used, and the Internet address of the site from which the user linked to the current site.

This type of information gathering is invisible and takes place without the user's knowledge or consent. Of course, users may also voluntaril disclose certain information—such as names, addresses, and telephone numbers—in order to access chat rooms or register for contests. Even voluntary disclosure carries risk, though, as the user has no way of knowing or controlling what happens to the information days, months, or even years after it is disclosed. One common scenario is that users' personal information is aggregated and exchanged among different marketing firms, which then target and contact potential customers.

While the privacy concern is currently quite significant, it will most likely worsen in the future. First, the Internet is growing at a breathtaking pace. The increase in the number of Internet users and data transmissions will only intensify the existing problem. Moreover, enhanced means of access to the Internet will likely change to make information exchange even easier, faster, and more uncontrollable. For example, television-ready interfaces now allow users to obtain high-speed access to the Internet through their television by use of a hand-held remote. If a user possessed a connection with a bandwidth sufficient to allow the transmission of high quality video, she could order movies and other programs from providers through this connection. If successful, one would expect this merger of television and Internet communications to generate vast new reservoirs of information, such as the movie preferences and viewing times of a particular user. This would also make many other types of information available to a potentially unlimited number of unknown third parties.

Second, an increase in the number of Internet users is likely to generate more Internet commerce. This translates to more online purchases and commonplace disclosures of sensitive data. Thus, there will be important economic reasons to quell consumers' fears about the privacy of their information. Consumer studies have shown that many consumers are wary about using the Internet because of information privacy concerns.[2] Under current law, those concerns are justified.

The third, and perhaps most invasive, concern is what can be termed the "monitoring problem." While the user chooses what pages to visit and what links to explore, it is the user's computer equipment and not the user herself who actually does the communicating. The monitoring problem exists because all online communications necessarily take place "behind the scenes." Therefore, the user faces the unavoidable problem of not knowing exactly what information has been provided by her Internet browser.

At first, the monitoring problem seems of little consequence. Most users would rightly assume that the producer of a commercial Internet browser, such as Netscape or Microsoft, would not communicate any information unless authorized. But most fail to realize that software other than the main browser is engaged during Internet communications. These additional pieces of software are commonly known as "plug-ins." Plug-ins can also transfer information to and from the user's computer, usually for specific purposes. Examples of plug-ins are a stock ticker which continuously displays the price of certain investments, a program which displays the current weather, or a sports score updater.

With plug-ins, a single Internet connection may begin to resemble a busy eight-lane freeway; it is no longer clear who, or what, is controlling the communication. Nor does the user know *exactly* what information is being sent from her computer. The Internet browser or plug-in performs this function based on the

user's commands and the data that has been encoded in the software by the publisher. Therefore, unlike in a spoken conversation, the user in an Internet communication does not exercise direct control over the signals being sent on her behalf. If designed properly, the browser or plug-in could access other data stored on the user's computer, information never intended to be disclosed to anyone.

Imagine a scenario in which a computer microprocessor manufacturer chooses to digitally mark each of its processors with a unique code number.[3] Therefore, each computer sold with that company's processor will have its own digital "fingerprint." If this code number was transmitted by Internet software, the user's "fingerprint" would stick to every site the user visited. Privacy would disappear at the moment the user goes online.

> This type of online snooping and information gathering is legal. Indeed, on the Internet it seems that nearly everything is fair game.

THE EXISTING LAW'S FEEBLE PROTECTION

> [O]n the Internet, new forms of criminal activity involving child pornography and pedophilia, assumed and fraudulent identification, sham billings and invasion of privacy are occurring at a rate faster than legislators can effectively devise solutions at both the national and state levels. Admit-tedly, specific and detailed legislation is necessary to deal with these crimes, but the law frequently has resorted to broad non-specific legislation to prevent commission with impunity until a solution is found. [4]

These words of the Superior Court of Pennsylvania strike at the heart of the problem. It is widely recognized that the current state of online protections—whether statutory, common law, or self-regulation imposed by the private sector—is insufficient to safeguard consumer privacy. However, there does not seem to be a consensus of opinion as to the most efficient way to achieve this end result.

On October 19, 1998, Congress passed the Children's Online Privacy Protection Act, the first law aimed at protecting online privacy.[5] This enforcement of the Children's Online Privacy Protection Act was preliminarily enjoined on February 1, 1999.[6] This law required websites to obtain "verifiable parental consent for the collection, use, or disclosure of personal information from children."[7]

There is no comparable protection for adult consumers' personal information collected by businesses through an online medium. Instead, Congress has left it to the private sector to regulate itself. When a consumer does resort to the courts to safeguard personal privacy, however, she is generally left without an adequate cause of action. For instance, in Jessup-Morgan v. America Online, Inc.,[8] the plaintiff brought suit against her Internet service provider America Online (AOL), because AOL provided her name and other personal information to another subscriber. AOL gave out this information in response to a subpoena served in connection with a civil lawsuit between the plaintiff and another party, about whom the plaintiff anonymously posted allegedly defamatory material.[9] In addition to several state law claims, including breach of contract and invasion of privacy, the plaintiff alleged that AOL violated the Electronic Communication Privacy Act (ECPA).[10]

The plaintiff attempted to invoke the ECPA, which prohibits disclosure of the contents of an electronic communication to any person or entity absent the occurrence of certain conditions.[11] However, the court found the ECPA to be inapplicable to these facts. The statute expressly defines "contents," as applied to electronic communications, to include "any information concerning the substance, purport, or meaning of that communication."[12] The court noted that information concerning the name or identity of a communication's author is not prohibited by the ECPA.[13] In fact, disclosure is expressly authorized by 18 U.S.C. §2703(c)(1)(A) (1998), which states:

> Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this sec-

tion) to any person other than a governmental entity.

On this basis, the court dismissed the plaintiff's ECPA claim.[14]

Breach of contract, breach of warranty, and claims of fraud can provide some relief to consumers. The success of these claims, however, turns on whether the Internet provider has represented that personal information collected from the subscriber will not be used for certain purposes, and yet takes actions inconsistent with that representation. Likewise, contract or fraud claims will provide little or no protection without any express or implied representations of confidentiality.

Even without specific privacy legislation, the Federal Trade Commission (FTC) has shown a willingness to police the collection and use of consumer information over the Internet through §5 of the FTC Act, which gives the FTC authority over "unfair" and "deceptive" trade practices.[15] In the absence of a privacy statute prohibiting certain uses of a consumer's personal information, the FTC's authority will likely be invoked only when a provider misrepresents one of its privacy policies to a consumer.

On August 13, 1998, the FTC released a complaint and agreement containing a consent order that illustrates how the FTC attempts to regulate this field under its authority. The agency alleged certain deceptive trade practices by Geocities, a provider and website operator. According to the complaint, Geocities represented to consumers that the information they provided would not be shared with third parties, unless consumers specifically indicated an interest in that third party's products or services.[16] Nevertheless, Geocites allegedly provided this information to third parties. The consent order stated that (1) Geocities would no longer engage in deceptive practices involving the collection or dissemination of private consumer information, (2) Geocities must thereafter obtain consent from parents of minors before releasing this information to any third party, and (3) Geocities must make certain disclosures to its users regarding its collection of personal information.

Specifically, Geocities must now disclose these matters: what information is being collected; the intended use(s) of the information; the types of third parties to whom it will be disclosed, whether advertisers, mailing list companies, the public, or others; the means by which consumers can access their own information as collected; the consumer's ability to directly remove or have that information removed from respondent's databases; and the procedures to delete personal identifying information from Geocities' databases and any limitations related to such deletion.

Outside this narrow provider misrepresentation context, the FTC is without regulatory authority. This void has not been filled; legislatures and courts have both been silent.[17] This lack of cases can be attributed to two chief factors: (1) this problem is not serious or widespread enough to prompt consumers to vindicate their rights or (2) the problem may be serious and widespread, but consumers cannot file lawsuits because they have no adequate cause of action. Developments in other countries demonstrate that this second reason is at the root of the problem. While American lawmakers have neglected the need for online privacy, their European counterparts have responded.

STATUTORY INTERVENTION OR PRIVATE REGULATION?

The gap in opinion between the proponents of statutory enactments and those of private industry regulation has recently grown more pronounced as a result of the European Union (E.U.) Council of Ministers' Directive on Personal Data, which binds all E.U. member nations.[18] This Directive requires that consumers must give their consent before any information about them may be processed by another. Further, consumers must be told that information is being collected, and how it will be used.[19] Certain classes of sensitive information, such as a person's race, ethnicity, health, sex life, and religious or political beliefs, may not be processed.[20] In addition, each member country must appoint an independent government authority to oversee the activities of companies that process personal information.[21]

The most far-reaching measure of the Directive requires that, as of October 25, 1998, each country prohibit the transfer of information to countries without an "adequate level of protection." To determine whether a country's level of protection is "adequate," the Directive considers both the substantive rules and enforcement mechanisms of challenged countries. The obvious implications of this transfer prohibition have fueled speculations of a "cyber trade war."[22] As of February 1999, the E.U. and the United States had postponed the pending "war," but they had not arrived at a satisfactory solution to the countries' differences.[23] This difference can be reconciled only if (1) the American private sector voluntarily sets up an adequate framework of protection guidelines and enforcement mechanisms, or (2) Congress enacts legislation to govern this uncertain area.

At this time, President Clinton clearly favors a market-led initiative to protect consumers' private information. On May 18, 1998, President

Clinton stated that he and the Japanese Prime Minister had agreed to move forward with a "market-oriented, private-sector-led approach to enhance privacy, protect intellectual property, and encourage the free flow of information and commerce on the Internet."[24] And on December 1, 1998, President Clinton again announced his intention that the Internet be self-regulated.[25] The Clinton administration has cautioned, however, that if the private industry cannot develop "effective privacy protection," the administration would reconsider its preference for self-regulation.[26] Ira Magaziner, senior advisor to President Clinton on Internet issues, believes that the United States will soon meet the requirements of the E.U. Directive through self-regulation.[27]

The Internet industry would likely embrace such a scheme of self-regulation. An adequate system of protection for personal information would only increase the number of online users and buyers. In a recent study, non-Internet users cited their concern over privacy as the main reason they were staying off the Internet.[28] Among Internet users, 81 percent were concerned about threats to their personal privacy.[29]

This growing concern has been reflected in the recent actions of several U.S. companies. The American company, NCR, an international leader in the area of data warehouse software, has announced a set of initiatives that will enable its clients to meet or exceed the European Union's privacy requirements.[30] According to NCR, new features of its data warehouse software will permit consumers to opt out of personal data collection, obtain reports on the type and use of data being collected, and correct information already gathered.[31]

In addition, the leading website operators have begun an online campaign to promote personal privacy on the Internet.[32] These website operators—America Online, Excite, Infoseek, Lycos, Netscape, Snap, and Yahoo! together claim to reach nine out of ten Internet users. Their campaign hopes to encourage companies to adopt such privacy policies as revealing their use of personal data and obtaining the prior consent of individual users.[33]

Despite this initiative by the private sector, international negotiations have so far failed to convince European officials that American safeguards can adequately secure consumer privacy.[34] The E.U. wants further assurances that computer users will have the right of access to their personal data and the right to redress if they suffer damage because the information is misused.[35] The E.U. insists that an independent arbitrator decide on such damage claims.[36] Steve Lucas, a member of the U.S. delegation to the E.U. Directive, has noted his "serious doubts" that the E.U. would accept the self-regulation schemes currently proposed by U.S. business groups.[37]

Opponents of statute-based privacy protections argue that the concerns of consumers can be handled most effectively by private industry. These opponents rely principally on the "laissez-faire" belief that the government should not interfere in areas of the economy that can be regulated through private initiative. Despite this argument, several factors tip the scales in favor of a statutory scheme.

A STATUTORY SCHEME MAKES SENSE

The first reason for a statutory solution concerns the manner in which the user's privacy is invaded. Often, personal information about consumers is taken without their knowledge. A consumer may never know that a certain website has taken information and distributed it to third parties. Only when consumers know that they have been harmed can they effectively address their concerns with "watchdog" groups or pursue legal remedies. But when the harm is dealt without witness or awareness, the single consumer or small group can hardly pursue these companies secretly violating industry standards.

If the appropriate guidelines were statutory, however, and enforceable by an agency such as the FTC, providers would be much more reluctant to exploit the unaware. The FTC would be in a far better position to investigate alleged violations and file complaints against providers that violate consumer privacy statutes.

A second reason for a statu-

ADDITIONAL RESOURCES ON INTERNET PRIVACY:

The Electronic Privacy Information Center

The Federal Trade Commission's Privacy Page

The Privacy Rights Clearinghouse

The Techlaw Journal

tory scheme, related to the first, is the inefficiency of the enforcement mechanism behind a privately initiated privacy standard. Without a legislative answer, it is unclear what remedy consumers could seek in the event of a "violation" by a provider. This difficulty stems from the nature of the Internet itself. Because the Internet is so decentralized, its agility allows and even encourages users to rapidly jump between "links" on webpages to display pages that are stored on different computers owned by different businesses. In addition, an Internet user usually has several different connections open at the same time. For example, a user may be viewing one page while he or she is simultaneously exchanging information with another entity, such as an advertisement found on the webpage currently displayed. As technology and connection speeds advance even further, it is likely that the number and nature of simultaneous connections will increase dramatically. Industry protections could hardly keep up.

Any private enforcement mechanism would have to be contractually based to create some representation of privacy on behalf of the website. However, it would be impractical and inefficient for an Internet user to digitally "sign" an information use agreement with every entity with whom information is exchanged. Even if this were possible, a challenging provider could litigate a myriad of issues relating to the validity of the contract with the user. The expense of such litigation would likely discourage consumers from bringing contract-based claims against providers. Therefore, Internet users would be resigned to browse without protest as they are exploited by online entities.

> Consumers must have confidence in their online privacy for the Internet to reach its full potential. A privately initiated protection system, with a toothless enforcement entity, will not inspire such confidence.

By analogy, these concerns resemble similar consumer-based concerns that were remedied by passage of the Fair Debt Collection Practices Act.[38] The purpose of that Act was to eliminate abusive debt collection practices.[39] The Fair Debt Collection Practices Act gave consumers a readily available means to vindicate their rights against businesses which took advantage of them, very similar to the purposes that would be served by an online privacy protection law. Just as consumers should be protected from unfair leverage in a debt collection situation, they should also be protected in cyberspace, where powerful companies build the machines, program the software, and control the networks.

A third factor that compels a statutory scheme is consumer confidence in online privacy. In order for the Internet to reach its full potential as a medium of interstate commerce, consumers have to be reassured about the level of privacy that they will enjoy. It is unlikely that a privately initiated protection system, with a toothless enforcement entity, will inspire such confidence in consumers.

The Children's Online Protection Act of 1998 provides much-needed protection to the integrity of personal information about children. Children are incapable of making informed and intelligent choices about the information that should be provided to online operators. Adults are in a very similar situation as they have no way of knowing when information is being collected. As a result, Congress should also extend consumer information protection to the entire public.

LEGAL INGREDIENTS FOR MAKING NEW LAW

The only law that Congress has enacted in this area is the Children's Online Privacy Protection Act of 1998. Section 1303(a)(1) states:

> It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).[40]

Section 1303(b) then provides that, within a year from enactment, the Federal Trade Commission must provide regulations which establish certain safeguards. Those regula-

tions must require the website operators to post notices that they collect information from children; obtain verifiable parental consent for the collection, use, or disclosure of personal information; and maintain reasonable internal policies and guidelines with respect to information gathering. Section 1303(c) treats a violation of this Act as an unfair or deceptive practice prescribed under §18(a)(1)(B) of the Federal Trade Commission Act.[41] States may also bring actions, pursuant to §1305(a)(1), in order to recover damages suffered by residents of that state as a result of any violation of an FTC regulation promulgated under §1303.[42] The remedies available under the Act include both injunctive relief and damage awards.[43]

Other than this Act, several bills have been introduced into Congress that recognized the need for statutory protections of consumers' private information. Though these proposals never became law, they nevertheless suggest increasing legislative support for a comprehensive statute.

The proposed Data Privacy Act called for the online computer industry to enact certain guidelines to protect consumers.[44] Under its provisions, the providers would notify the user that information is being collected, the nature of that information, and that the user has the option to prohibit disclosure of the information.[45] This notice would be provided before or at the same time the data is collected. At the request of the user, the providers must further provide a description of third party recipients of the information, allowing the user to verify the information and correct any errors.[46]

The proposed Communications Privacy and Consumer Empowerment Act called for FTC rules that mandated that consumers be informed that information is being collected about them, that users receive conspicuous notice that the collected information could be used or sold to a third party, and that providers "exercise control over the collection of personal information and to stop the unauthorized use, reuse, disclosure or sale of that information."[47] The proposed act also contained findings of fact. One such finding stated that further protections are needed to ensure that consumers' rights are "retained and respected" by other entities doing business in cyberspace.[48] The proposed Act also estimated that some five million young Americans used the Internet and that this number was expected to triple by the year 2000.[49]

Before enacting online consumer protection legislation, Congress must first decide what exactly is to be protected. On one hand, it is vital to the functioning of the Internet that businesses be able to collect information from consumers. On the other hand, the individual consumer lacks the awareness and resources to challenge exploitative collection. The difficult task is to design legislation which puts consumers on a level playing field with the online businesses. Ideally, online businesses should be prohibited from taking "personal" information from consumers without their knowledge.

But this is not as simple as it sounds. First, Congress must precisely define "personal information." Any definition will most likely contain ambiguities. It would not be prudent to ban the collection of *every* type of information because the Internet necessarily requires transmissions of certain data as part of every communication. For example, every connection requires a commercial operator to identify the computer network from which a user has connected so that responses can be sent to the correct part of the Internet. This type of identifying information must be collected.

In contrast, an operator would have little, if any, justification for extracting information which is stored on the user's computer. One response may be to draft language allowing operators to collect, without the user's consent, only information "necessary and vital to the operation of Internet communications and the common protocols which are embodied therein." This language is still broad but could be effectively narrowed by rules and regulations promulgated by an agency having jurisdiction over the execution of the law, such as the FTC, or by judicial interpretation.

> Unlike face-to-face conversations, the Internet involves communications between invisible parties who are not actually exercising control over all aspects of their communication.

A second hurdle to uniform legislation is the presence of "limited-purpose information." This data the consumer has willingly supplied to a commercial operator for a limited transaction, such as credit card information, names, addresses, telephone numbers, e-mail addresses, and the like. This supply of information, however, should not enable commercial operators to further appropriate the information for purposes beyond the scope of the original transmission. The statute should establish guidelines requiring commercial operators to obtain consent from the users for any non-implied uses of the information, or, alternatively, grant the FTC jurisdiction to promulgate its own guidelines. Because of the ephemeral nature of the medium, there will most likely be evidentiary disputes over whether the user, for example, clicked the "Yes" button to allow the operator to use her information in a certain manner. For this reason, the guidelines should require the operators to obtain consent through a somewhat more stable forum, such as an e-mail from the user.

Another wildcard concerns the federal agency which should be given enforcement authority over the terms of an Internet privacy law. It is unlikely that existing knowledge of the relationship between consumers and commercial entities will be sufficient to allow any agency to understand the dynamics of the cyberspace environment. Unlike television and radio, the Internet is a two-way communication that may not be occurring on a large scale environment. And, unlike face-to-face conversations, the Internet involves communications between invisible parties who, as already discussed, are not actually exercising control over all aspects of their communication. Therefore, it may be appropriate to develop another administrative division, such as a Department of the Internet (DOI), which may exercise its authority from within a parent organization, such as the FTC or FCC. Much akin to the Antitrust Division of the Justice Department, the DOI would contain a staff of experts who would enforce Internet regulations and promulgate rules on behalf of the FTC or FCC. The DOI division would be able to respond to rapidly developing, complex Internet issues, something the FTC or FCC, as a whole, may not be able to do.

The world of cyberspace is, in some respects, similar to the business world that we all inhabit and create with every transaction. It revolves around the transfer of information between parties. In many other respects, however, cyberspace is dramatically different. Once online, one cannot monitor the behavior of the parties with whom one deals; indeed, one cannot even monitor the behavior of one's own agent, the computer. This lack of awareness and control leaves the consumer vulnerable, without the incentive or even ability to guard against exploitation by others.

The explosion in popularity and utility of the Internet has created the unique world of cyberspace. Not surprisingly, the creation of this new forum has also brought equally unique and unforeseen problems. Consumers are adrift in this strange new universe and cannot be expected to defend themselves, using technology they may not understand, against predators they cannot fully perceive. Congress should act now, before the nation becomes even more dependent on online communications. The government must protect consumers from the biggest black hole in cyberspace—the consumption and misuse of personal information. ◆

"As the Internet is still in its relative infancy, Congress would serve the public—and the cause of fostering greater electronic commerce—by putting basic privacy protections on the books this year."

—Rep. Edward Markey (D-Mass.), ranking member of the Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection

Source: *Internet Users Need Privacy Bill of Rights*, ROLL CALL, Feb. 22, 1999.

[1] Reno v. ACLU, 117 S.Ct. 2329, 2334 (1997) (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

[2] Louise Kehoe, *US Campaigners For Privacy To Go Online*, FINANCIAL TIMES (London), Oct. 7, 1998, *available in* LEXIS, News Library, Fintme File.

[3] This scenario is not entirely hypothetical. The Intel Corporation recently caused a stir when it proposed new Pentium III™ processor chips with the capability to transmit unique identification number without user approval. Upon objection by privacy groups, Intel responded by providing the user the ability to disable this identification feature. Jeri Clausing, *Privacy Advocates Ask FTC To Force Recall of Intel Chips*, N.Y. TIMES, Jan. 29, 1999, at C3.

[4] Commonwealth of Pennsylvania v. Vida, 715 A.2d 1180, 1184 (Pa. Super. Ct. 1998).

[5] Children's Online Privacy Protection Act, Pub. L. 105-277, §1301 et seq., 112 Stat. 2681 (1998).

[6] ACLU v. Reno, 1999 U.S. Dist. LEXIS 735 (E.D. Pa. Feb. 1, 1999) (enjoining the Act's prohibitions against distribution of material "harmful" to minors, but refusing to enjoin other provisions of the Act).

[7] §1303(b)(1)(A)(ii), 112 Stat. 2681, 2681-733.

[8] Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998).

[9] Id.

[10] Id.

[11] "A person or entity may divulge the contents of a communication —(1) to an addressee or intended recipient of such communication ... (3) with the lawful consent of the originator or an addressee or intended recipient of such communication ... (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or (6) to a law enforcement agency ... (A) if the contents (i) were inadvertently obtained by the service provider; and ... appear to pertain to the commission of a crime[.]" Electronic Communications Privacy Act, 18 U.S.C. §2702(b) (1998).

[12] 18 U.S.C. §2510 (1996).

[13] Jessup-Morgan, 20 F. Supp. 2d at 1108.

[14] Id.

[15] Federal Trade Commission Act, §15, 15 U.S.C. §45 (1994).

[16] In re Geocities, 1998 FTC LEXIS 92 (Aug. 13, 1998).

[17] On Oct. 15, 1998, this author searched each of the comprehensive federal and state case law databases on LEXIS and Westlaw for cases containing the word "Internet" within the same sentence as "privacy" with no date restriction. Out of the relatively few cases returned, only Jessup-Morgan was applicable to this topic.

[18] Mark E. Budnitz, *Privacy Protection For Consumer Transactions In Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847, 868 (1998).

[19] Id.

[20] Id.

[21] Id.

[22] Louise Kehoe, *US, EU In Bid To Avoid 'Cyber War'*, FINANCIAL TIMES (London), Aug. 28, 1998, *available in* LEXIS, News Library, Fintme File.

[23] *Net Commerce*, FINANCIAL TIMES (London), Dec. 3, 1998, *available in* LEXIS, News Library, Fintme File.

[24] Remarks at the World Trade Organization in Geneva, Switzerland, 34 WEEKLY COMP. PRES. DOC. 926 (May 18, 1998).

[25] Mark Suzman, *Electronic Commerce White House Backs Self Regulation: Clinton's Boost For The Digital Economy*, FINANCIAL TIMES (London), Dec. 1, 1998, *available in* LEXIS, News Library, Fintme File.

[26] Budnitz, *supra* note 18, at 67-68.

[27] Kehoe, *supra* note 22.

[28] Kehoe, *supra* note 2.

[29] Id.

[30] Paul Taylor, *Boost For Consumer Privacy*, FINANCIAL TIMES (London), Oct. 12, 1998, *available in* LEXIS, News Library, Fintme File.

[31] Id.

[32] Kehoe, *supra* note 2.

[33] Id.

[34] Emma Tucker, *Deadlock in US-EU Talks On Data Law*, FINANCIAL TIMES (London), Oct. 8, 1998, *available in* LEXIS, News Library, Fintme File.

[35] Id.

[36] Id.

[37] Kehoe, *supra* note 2.

[38] 15 U.S.C. §1692 (1994).

[39] 15 U.S.C. §1692(e).

[40] §1303(a)(1), 112 Stat. at 2730.

[41] §1303(c), 112 Stat. at 2732.

[42] §1305(a)(1), 112 Stat. at 2733.

[43] Id.

[44] H.R. 2368, 105th Cong. (1997).

[45] Id.

[46] Id.

[47] H.R. 1964, 105th Cong. (1997).

[48] Id.

[49] Id.