Journal of **Multistate Taxation**
September, 2001

Sales and Use Taxes

PRIVACY ISSUES MAY ADD TO THE DEBATE OVER STATE TAXATION OF E-COMMERCE

Phillip W. Gillet, Jr. [FNa1]

The most significant characteristic of privacy and Internet taxation seems to be that there is no consensus on the proper actions needed to protect revenue, privacy, and the growth of the Internet.

At the dawn of a new millennium, the leaders of the western (i.e., industrialized) world scrape to solidify their position atop the global information society and world economic hierarchy by capturing the lead in what many see as the economic crown jewel of the 21st Century--electronic commerce. [FN1] The borderless features of cyberspace create much of the excitement and mystique associated with e-commerce. The Internet allows merchants and consumers with a computer and a communication system to transmit anywhere, and almost instantly, digital information including credit card numbers and other payment and ordering data. [FN2] Therefore, "[t]he Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location." [FN3]

E-commerce's strength lies in its elimination of some previously prohibitive costs and overhead that accompany business transactions. [FN4] These prohibitive costs uniquely hamper small businesses and consumers, who typically lack the economies of scale that big business enjoys. Along with this strength comes one of e-commerce's biggest problems: the relative ease and small cost of collecting, maintaining, and storing vast quantities of information about Web surfers (including, e.g., who and where consumers are, their buying habits, Web sites frequented, and education, health, and credit history). Modern information "spies" sell their espionage about Web surfers. Businesses hoping to become cyberspace "rulers" hire these information- collecting "spies" and use the personal information to strategically tout their wares before "the rest of the people['s] ... normal eyes." [FN5]

For example, when a subscriber logs on to a Web site, frequently the subscriber's name appears at the top of the screen. The company knows who the subscriber is because the individual has provided--presumably willingly--such information as his name, address, and other data, perhaps including various personal preferences. This seems simple on the surface but what goes on behind the scenes may be surprising. The Web site's information spies can find out the name of the company through which the subscriber accesses the Internet and what pages the subscriber views and for how long. In addition, the Web site can determine the particular types of items that are viewed, and can collect and analyze this data and, accordingly, send strategically marketed information or advertising banners. [FN6] Some Web sites assert ownership over their customers' personal information. For instance, Amazon.com, Inc. posted such a notice on its Web site, claiming the information was the company's "transferable asset." [FN7]

Who are these spies and how can they be seen? In fact, they are computers compiling and analyzing massive volumes of information. This type of data collection creates many novel, hotly debated privacy issues, as can be seen by the myriad pages of magazines, journals, and books consumed with these issues.

American privacy laws have long differed from those of the rest of the world. Most countries see privacy as a basic human right. [FN8] Under American jurisprudence, privacy rights are only one part of the American "bundle of rights." [FN9]

Taxation issues.

Another equally important and hotly debated cyberspace issue is the imposition of state and local sales and use taxes on e-commerce. Currently, e- commerce generally is taxed to the same extent as traditional mail-order purchases. For example, a state or local jurisdiction can require a vendor to collect its sales tax only if the vendor has a significant connection, or nexus, with the state. This connection generally requires that the vendor have a physical presence in the taxing state. [FN10] Some state and local governments, recognizing the detrimental effects that a robust "e-conomy" could have on their tax revenues, have begun to express concern over the Internet taxation moratorium created by the Internet Tax Freedom Act. [FN11]

Taxation and privacy. Contemplating the taxation of these new and rapidly advancing types of transactions gives rise also to privacy concerns. In that regard, it is useful to examine the effect of differing views on privacy and the impact of e-commerce taxation on American companies selling their goods via the Internet. While the Internet and the "information age" have created a variety of privacy issues, the scope of this article will be limited to the collection, retention, and distribution of personal information collected by private companies for taxation purposes. Specifically, how will the collection of sales and use taxes affect consumers' personal information privacy? That this topic has received little scholarly or governmental attention seems strange given that the Federal Trade Commission "has been involved in addressing online privacy issues for almost as long as there has been an online marketplace...." [FN12]

The discussion of the e-commerce tax framework will be limited here to sales and use taxes. [FN13] Also, to effectively analyze these issues a basic understanding of the history and legal framework of e-commerce is necessary, along with some knowledge regarding the various information collection devices and the laws protecting privacy in the U.S. In the end, this analysis generally will show that privacy concerns are relatively inconsequential in relation to taxation of e-commerce because of the minimal additional intrusion on e-commerce as a result of assessing and collecting sales and use taxes.

Sales and Use Taxation of E-Commerce

Most states impose a tax on retail sales transactions. Some states, such as California, impose the tax on the seller for the privilege of making retail sales in the jurisdiction. Sellers can seek reimbursement for sales taxes from buyers but the sellers ultimately are responsible for the tax liability created by the sale. [FN14]

States are limited by constitutional constraints in taxing all sales originating or commencing within their borders. Specifically, significant jurisdictional issues arise when transactions occur between a seller in one state and a buyer in another. The seller's state may not impose a gross receipts tax on sales to customers in other states. [FN15] The buyer's state cannot impose its sales tax on sales originating in other states. [FN16] Therefore, many mail-order--and now e-commerce--transactions between buyers and sellers in different states avoid state sales tax.

To recapture this lost sales tax revenue, some states impose a use tax for the privilege of using taxable property in the state. The duty to pay use tax is on the buyer. This approach catches the tax avoided by a state's citizens' buying goods from out-of-state sellers. The U.S. Supreme Court has upheld the imposition of use taxes on interstate transactions. [FN17] One problem with use taxes is that enforcement on buyers is such a logistical nightmare that states rarely actively enforce their use tax provisions. Nevertheless, an out- of-state seller with sufficient nexus with the taxing state can be compelled to collect use taxes for sales delivered in the state. [FN18] While this situation solves some of the logistical problems with collecting a use tax, much use tax liability remains uncollected.

State sales and use tax primacy.

State and local taxing systems across the U.S. are quite similar in their overall structure and concepts. Historically, state governments enjoyed virtually complete autonomy in determining the goods and services that were taxable. [FN19] Thus, it may seem curious that the states' taxing systems developed similar structures and concepts.

The original colonial taxing systems varied significantly among the states, depending on their geographical location. [FN20] These differences resulted from the varied economic structures of the colonies. For example, colonies in the North, with their mercantile systems, had different objectives than the plantation owners of the South. The colonies' taxing systems developed based on social and economic conditions; by the late 18th Century, the property tax was the main source of state revenue and it remained that way until the early 1900s. [FN21] Eventually, the states' need for revenue made them shift their focus to the more lucrative individual income taxes, motor vehicle and gasoline taxes, "sin" taxes, and general sales taxes. This shift in focus, and the states' difficulty in overseeing local property taxes, allowed local governments and school districts to step in and line their revenue coffers with the property taxes.

While the state taxing systems are similar in structure and concepts, the more detailed workings, however, are quite different. Local history and politics played a large role in the development of the differences. [FN22] These differences create potential tax savings opportunities through careful management of state and local tax liabilities. Until recent years, U.S. companies often considered state and local taxes as simply a cost of doing business. [FN23] Their strategic planning was based on market conditions rather than tax status. Today, most multistate companies "realize that state and local taxes can be managed, and that every dollar of state and local tax saved, net of the federal income tax effect, goes straight to the bottom line." [FN24] In general, the significance of state and local taxes should not be underestimated; many U.S. companies pay more state and local taxes than federal taxes. [FN25] Accordingly, there has been an explosion in state and local taxation planning.

The tradition of federalism and states' rights is seen in the U.S. Constitution's recognizing the states' freedom to determine and administer tax rates and bases. The states are given autonomy in this area. At the same time, the federal government is authorized under the Commerce Clause of the U.S. Constitution to regulate interstate commerce. [FN26] The federal government seems to intervene when either significant political or significant financial stakes exist.

In the global debate on the taxation of e-commerce, no issue has received more attention than state sales and use taxes in the U.S. [FN27] The primary reason for this heated debate likely stems from the perceived significant financial stakes. Sales and use taxes provide the states with a very significant source of revenue, and anything that potentially threatens this revenue is of great concern to state and local taxing authorities.

Some studies estimate that between 1998 and 1999, online sales doubled to $20 billion, and by 2002 they will exceed $300 billion. [FN28] Based on that $300 billion projection, state and local governments may lose as much as $20 billion in uncollected Internet sales taxes by 2002. A seemingly more realistic prediction, however, expects e-commerce to generate $40 billion by 2002. [FN29] Thus, the potential revenues generated by e-commerce would be significantly less material; e-commerce would represent only 1.28% of all retail sales. [FN30] In addition, based on these lower projections, state and local governments would lose only about $2 billion in taxes, a relatively immaterial sum in the overall scheme of state and local revenues.

As a result of this perceived importance, various e-commerce initiatives have focused primarily on sales and use taxes, including the Internet Tax Freedom Act, the federal Advisory Commission on Electronic Commerce (established under the ITFA), and the National Tax Association's Communications and Electronic Commerce Tax Project. [FN31] In addition, most discussions relating to other types of taxes have been framed using sales and use tax concepts and problems. Besides the significant financial motivation, this focus is due also to the complexity of sales and use taxation resulting from widely varying state and local tax schemes.

The states maintain the only U.S. broad-based sales tax. In addition, sales and use taxes in a multijurisdictional environment often provide the greatest enforcement difficulty. Finally, the U.S. has a significantly greater number of state, county, and local jurisdictions imposing sales and use taxes than do most other industrialized nations. [FN32]

Therefore, the jurisdictional and collection issues apply to a very geographically diverse group of state citizens, thus increasing the collection and enforcement complexities.

Enforcement and collection problems.

States generally require sales or use tax collection by businesses making sales in the state that have a physical presence in the state--a relatively easy rule to enforce. Out-of-state e-businesses, however, cannot be forced to collect and remit state sales or use taxes because federal interstate commerce laws generally prohibit states from exercising tax authority beyond their physical borders. [FN33] Even if Congress were to change the law to allow this type of taxation, it would be virtually impossible to effectively enforce the imposition of state and local sales taxes on out-of-state businesses delivering products into a taxing state.

The states, of course, may require their residents to report and pay taxes on items purchased from out-of-state vendors, i.e., the "use" tax. Taxpayers are frequently unaware of this requirement, however. In addition, the difficulty in enforcing the use tax further undermines its application. The states also do not make it easy for taxpayers to comply even if they want to. In California, for example, while no mention of the use tax is made on the state's personal income tax return, buried among the 68 pages of instructions, under "additional information," are directions concerning a taxpayer's liability for use taxes. Taxpayers are instructed to compute any use tax using the sales tax rate for their place of residence and to remit their payment to the State Board of Equalization along with their name, address, and a description of their purchases. [FN34]

The biggest barrier in use tax collection may be the general absence of a clear reporting mechanism, which makes noncompliance almost undetectable. Sellers have no use tax reporting requirements, and most states do not exhibit any real intent to require buyers to self-report. Given the obvious weaknesses in enforcement and collection, use taxes are not very popular. They generally remain in effect simply because they are on the books, while taxpayers are unaware of their existence.

To effectively collect all sales and use taxes, the states and localities must find a practical way to enforce the tax system. One initiative presently under way in this area is the Streamlined Sales Tax Project for the 21st Century (the SSTP), in which approximately 40 states are working to develop a simplified state tax system that would encourage voluntary tax collection by remote vendors. [FN35] The system would, in part, rely on one or more approved third-party clearinghouses to collect and remit taxes on remote sales. Moreover, for such a system to be mandatory rather than voluntary, statutory changes at the federal level would be needed because, as indicated above, the Commerce Clause of the U.S. Constitution precludes states from imposing tax- collection responsibility on out-of-state businesses. Some observers have noted that positive elements of the SSTP include that it (1) it eases the administrative burden for businesses, (2) avoids creating another federal bureaucracy, [FN36] and (3) allows technology to lead.

The SSTP's proposed third-party collection suffers from some of the same problems as traditional use tax collection. Each of the thousands of state and local taxing jurisdictions would need to keep the collection parties updated as to their current laws. Another significant problem is that the definition of what is taxable varies widely. For instance, 18 states charge sales tax on "clothing" but differ in their definitions of clothing. Therefore, this solution does not come without significant problems to be resolved.

One feasible solution might be the state cooperative approach suggested by one of the participants in the Advisory Commission on Electronic Commerce. [FN37] This approach employs a system similar to that for collection of the states' fuel use tax, which had similar problems to e-commerce. [FN38] Despite the logistical difficulties of the fuel use tax, the system works well. Therefore, implementing a similar system for e-commerce taxation could provide an effective collection method.

Historical Context of the Internet and E-Commerce

The Internet is by and large just a set of computer hardware and software standards that allow computers to exchange data with other computers. [FN39] The computers can be very close to each other, such as across the street, or very far apart, such as half way around the world, and they even can have incompatible operating systems. The standards allow any computer connected to the Internet to exchange information.

The birth of the Internet can be traced back to the Soviet Union's launch of the first Sputnik satellite in 1957. Concerned about losing the space race, the U.S. government created the Advanced Research Project Agency (ARPA) in 1969. [FN40] This project created a linked system of computers and computer networks owned and operated primarily by government agencies, defense contractors, and university laboratories. The network then evolved far beyond its humble origins in the U.S. to include universities, corporations, and individuals from around the world. From the Internet's inception, government, industry, and academia collaborated in its evolution and deployment. The history of the Internet revolves around four distinct aspects: (1) technological evolution, (2) operation and management, (3) social aspect, and finally (4) commercialization. [FN41]

No single entity administers the Internet. Rather, hundreds of thousands of separate, independent operators use common transfer protocols to communicate with other computers. The Internet is decentralized, in part, because of the technical unfeasibility of one entity's controlling all the information. [FN42] The "Worldwide Web" (or Web), [FN43] as we now know it, was born in 1989. The Web, a component of the Internet providing access through a user- friendly environment, "is a widespread information infrastructure, the initial prototype of what is often called the National (or Global or Galactic) Information Infrastructure." [FN44]

A key element of the rapid growth of the Internet has been free and open access. The system promoted quick dissemination of the long-practiced open publication of ideas and research in the academic community. This type of community spirit has been present for virtually all the Internet development. "The Internet is as much a collection of communities as a collection of technologies, and its success is largely attributable to both satisfying basic community needs as well as utilizing the community in an effective way to push the infrastructure forward." [FN45]

Many supporters of an Internet free of government intervention hypothesize that any regulation (e.g., privacy law or taxation) will stifle Internet expansion. Further, these people argue that the market should regulate itself, and that consumers' patronage, either by surfing or purchasing, will be the most efficient regulator of the Internet. They cite the Internet's self- regulation as the key to breaking down the traditional formalistic barriers in the exchange of ideas in the academic community. This self-regulation is also partly responsible for allowing innovation to create the modern e-commerce landscape. [FN46]

The final, and perhaps most significant, community to recognize the Internet's value was the commercial sector. The rapid growth in the commercial sector caused increased concern over developing a homogeneous communication standard. Despite the Internet's growing beyond its initial humble beginnings, users still appreciate, and want to continue, open and fair access. "The Internet has changed much in the two decades since it came intoexistence.... [I]t started as the creation of a small band of dedicated researchers, and has grown to be a commercial success with billions of dollars of annual investment." [FN47]

Privacy in Cyberspace

Many people may not realize the importance of--and lack of--privacy protection on the Internet. Some privacy advocates have claimed that "Internet privacy" is "an oxymoron in progress." [FN48] For example, a widely respected career Air Force Colonel with more than 25 years of service was court marshalled in connection with the contents of his private e-mail account. [FN49] The Colonel had initiated a subscription to America Online (AOL) some time well before the alleged violation of military law. He paid for his computer and the software and accessories with his personal funds. Three pictures downloaded from the Colonel's computer were admitted as evidence of child pornography. Although the military court ruled that an expectation of privacy existed in e-mail, this finding is certainly not binding on civilian courts. E-mail, Web surfing habits, [FN50] and other information could be obtained from an individual's computer and used in a criminal or civil action.

Every time someone connects to the Internet and accesses the Web, information about that person and the person's surfing habits is probably being collected. [FN51] This occurs through direct methods, such as voluntarily filling out forms or otherwise submitting information, as well as by indirect methods. Most surfers have no idea that without their consent, Web sites are harvesting such personal information, primarily via "click stream" data [FN52] and "cookies." [FN53]

Internet service providers (ISPs) collect and maintain click stream data each time a user surfs the Web. The ISPs may maintain records of each Web site visited, e-mail communication, advertisements viewed, purchases made, and other online activity. Typically, this information is collected without the user's permission or knowledge; the accumulation of click stream data goes on silently without much fanfare. In addition, most ISPs do not divulge what click stream data they collect and what they do with it. [FN54]

Data also is collected by sending cookies from the Web site to the surfers' computers. Cookies generally enter the computers unannounced, unless the Web surfers appropriately configure their browsers to not accept cookies. [FN55] The cookies allow individual Web sites to gather information about surfers. Each hit on the Web site by a surfer can provide the site operator with valuable data that can be sold or used to increase profits. [FN56] Some ISPs allow users to set their browsers to alert them each time a Web site attempts to send them a cookie. [FN57] The surfer may accept or refuse the cookie and then, regardless of the choice, is allowed to enter the Web site.

Nevertheless, cookies can add value to the surfers' Web experience. Many Internet businesses are investing heavily into improving the shopper's experience and expanding into new markets. [FN58] For example, a Web site can use cookies to maintain a list of a surfer's preferences from previous visits, thus customizing the site for subsequentvisits. [FN59] At the same time, the cookies allow Web sites to develop profiles of their surfers, probably benefiting the Web site far more than the surfer. Thus, Web sites can both collect information and serve customers' wants and needs better with the aid of cookies.

One downside of collecting and compiling this information is that sometimes security breaches occur, allowing others to view personal information. For example, Outpost.com, a Web site hawking high-tech gear, had a security glitch in its system that inadvertently allowed unauthorized persons to view customers' ordering information, such as e-mail addresses and order history. [FN60]

Whether the use of cookies constitutes an invasion of privacy, either criminally or in tort, has been the subject of much analysis. [FN61] Current cookie technology does not specifically identify a user; it just tracks the user's surfing habits and preferences. In addition, most Web sites have privacy disclosure sections that users either may visit or must click on in order to indicate agreement. Therefore, as long as Web sites do not violate their own contractual policy agreement, given the limited information collected, cookies as currently used likely would not be an invasion of privacy under federal law. [FN62] State law violations, however, may exist. [FN63]

Finally, as personal information collection becomes more complex, there may be federal privacy invasions. [FN64] Specifically, information exchanges between companies about a particular Internet user would seem to come very close to--if not actually--violating the federal privacy protections because such data collection would involve more than a single inquiry, and it also seems particularly repugnant to the underlying policy of Anglo-American privacy law. [FN65]

This user identification scenario is not too farfetched. Recently, each of Intel's Pentium III microprocessor chips was found to contain a unique "processor serial number" (PSN) that was transmitted with cookies. Thus, by using a matching service with the retailer or manufacturer's warranty registration database, the user could be identified and matched with volumes of cookie information. [FN66] A great expression of public concern over this situation, however, led Intel to quickly disable this function. Moreover, the other major chip providers likely will not attempt to do something like this soon, because the event created a public relations and marketing nightmare for Intel.

DoubleClick.com's matching its database of online profiles with Abacus's database of consumers' offline behavior has certainly created a stir among privacy advocates as well. [FN67] That type of action could provide an aggregated database that would profile consumers to an extent almost unimaginable just a few years ago. In addition, Web sites

could start using a uniform cookie system that would allow all companies to exchange data about a user's complete surfing habits. This would certainly create an Internet in which privacy was nearly absent.

Privacy Laws

Many world leaders perceive taking the lead in e-commerce as the key factor in leading the 21st Century economic landscape. [FN68] In 1998, then- President Clinton predicted that in just a few years, trade on the Internet would generate hundreds of billions of dollars in goods and services. [FN69] Despite Clinton's enthusiasm, he said e-commerce was, in many ways, the global economy's "Wild West," [FN70] where, as a couple of commentators noted, "some enterprising competitors may be willing to go in and make a quick buck before the sheriff shows up, but rest assured that the sheriff ... is on the way." [FN71] For e-commerce to flourish, a "safe and stable terrain for those who wish to trade on it" must be established. [FN72] Although the $9 billion of e-commerce in 1998 leaves a way to go to reach Clinton's prediction, it was still quite impressive, and in 1999 e-commerce soared to about $20 billion. [FN73] Also, between 1997 and 1998 the proportion of retailers selling on the Internet more than tripled--from 12% to 39%. [FN74] Online retail spending is growing at a rate of 70% annually,and only slightly more than one in ten Americans uses e-commerce to purchase goods and services. [FN75] Therefore, a tremendous upside potential exists; however, the growth of e-commerce has slowed. One seemingly realistic prediction, which, as noted above, expects e-commerce to generate $40 billion by 2002, also estimates that approximately $18 billion in revenues will be lost in that year because of privacy concerns. [FN76]

The tremendous upside potential of e-commerce has also sparked European countries to enter the race to lead cyberspace. In October 1997, the House of Lords (the British Parliament's upper house), feeling the fever to recapture the nation's long-gone position as the world's economic leader, held a debate on electronic commerce. One member of Parliament felt that e- commerce's infancy [FN77] would be short lived, and recognized the once-in- a-lifetime opportunity" of capturing the lead in this hot area. The member thought regulation was necessary to protect consumers, and noted that existing laws were continually being outdated by the rapid advances in technology. [FN78] This makes it "abundantly clear that the old frameworks just would not work." [FN79] The member's conclusions about protecting consumers seemed to be aimed at increasing Britain's share of e-commerce revenues.

In general, European laws protect privacy more than American laws, and many European nations are using the U.S.'s rather liberal privacy laws as a tool to hinder American e-commerce in Europe. The European Union member nations condemn American privacy laws, although they cite readily available public information as America's competitive advantage in the global market place. [FN80] Therefore, the possible foreign competition can be used as another reason to argue that the market, not the government, should regulate.

While Europeans' views on privacy law may be somewhat self-serving, [FN81] their observations about consumer concerns are quite correct. In a recent poll, consumer trust emerged as e-commerce's biggest barrier to growth. [FN82] According to a couple of commentators: "One of consumers' greatest fears is that by clicking "send," they have sent their personal financial information off into space, at the risk of being seen, copied, or misused." [FN83] Although financial information loss is an important consumer privacy issue, equally important is the involuntary collection of data about Web surfers. [FN84] Many consider this involuntary data collection to be the "dominant privacy issue on the Internet." [FN85] While some might see this as a rather minor problem, e-commerce consumers tend to be very fickle. [FN86] Therefore, the privacy problems might significantly hinder e-commerce from reaching its full potential.

Privacy's Anglo-American Legal Framework

Anglo-American jurisprudence first formally recognized the right to privacy near the end of the 19th century. A 110-year-old Harvard Law Review article warned that advances in technology could turn previously private details into public information. [FN87] These warnings seem very relevant today, and exploiting personal information may be seen as a relatively recent development. That is certainly not true, however. The fear of using technology to tap

into one's personal information has been present for well over 30 years. [FN88]

In the U.S., privacy rights in personal information are not specifically guaranteed in any set of law. Rather, this right is protected by a patchwork of federal and state constitutional, statutory, and case law. While recent surges in legislation regarding technology and privacy have occurred, to address the entire legal structure goes beyond the scope of this article. [FN89] A brief overview of the primary legal framework should prove sufficient here.

Constitutional and case law protections.

The U.S. Constitution recognizes no specific right to privacy. [FN90] In fact, the U.S. Supreme Court has said "the protection of a person's general right to privacy--his right to be left alone by other people--is, like the protection of his property and his very life, left largely to the law of the individual States." [FN91] The Supreme Court has held certain personal decisions beyond the reach of government. [FN92] The First [FN93] and Fourth [FN94] Amendments protect some types of information. Thus, although not explicitly stated, informational privacy likely would fall under the protection of the U.S. Constitution. Constitutional protections, however, generally apply only to governmental infringements. [FN95] Nevertheless, the Court has stated: "Although the conduct of private parties lies beyond the Constitution's scope in most instances, governmental authority may dominate an activity to such an extent that its participants must be deemed to act with the authority of the government and, as a result, be subject to constitutional restraints." [FN96] This idea could be used to argue that because the government founded and funded the Internet, the conduct of hosting an Internet Web page [FN97] or maintaining a Web site should be characterized as a state action. [FN98] Thus, these functions would be subject to the U.S. Constitution. At least one commentator, however, has argued that e-commerce is no more public than "real" transactions relying on the federal and state legal framework to keep them functioning. [FN99]

The Fourth Amendment. The Fourth Amendment protects against unreasonable searches and seizures. [FN100] The collecting of information through cookies andclick stream data without one's consent or knowledge could be categorized as an invasion of privacy. [FN101] This implicitly embodies the right to privacy from governmental intrusion. Therefore, private parties' information collecting would fall outside of the Fourth Amendment protections.

That technology's use causes novel legal concerns is certainly not new. The use of advanced technology in surveillance first clashed with the Constitution in Olmstead v. U.S. [FN102] There, the U.S. Supreme Court held that the Fourth Amendment provided no protection from the government's tapping the telephones of alleged conspirator's residences. The Court reasoned that the Fourth Amendment protected only "physical invasions" by the government. In Justice Brandeis's well-known dissent (where he expressed concern over the problem he had identified almost 40 years earlier [FN103]), he urged the court to broaden the notion of privacy. Justice Brandeis wanted the court to look at both "what has been ... [and] what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."

In Katz v. U.S., [FN104] the Supreme Court partially limited the Olmstead decision by holding that a person in a telephone booth may rely on the protection of the Fourth Amendment. The Court also abandoned the "physical intrusion" requirement of Olmstead, substituting a "reasonable expectation of privacy" standard. Using this standard, one could argue that using a computer in one's own home or office gives rise to a reasonable expectation of privacy, thus making involuntary data collection about Web surfers an actionable intrusion of privacy. [FN105]

Informational privacy. It took a few more years before the U.S. Supreme Court, in 1977, expressed its view on informational privacy. In Whalen v. Roe, [FN106] the Court held that individuals had a right to have their personal information protected by the government. Thus, one might argue that even if hosting Internet Web pages and maintaining Web sites are not governmental actions, the government must step in and protect the personal information of Web surfers.

More recently, U.S. v. Maxwell [FN107] questioned, before a military court, whether a reasonable expectation of

privacy existed in private e-mail. The trial court, relying on Katz, held that an Air Force colonel's sending and storing pornographic material through America Online came within the Fourth Amendment's reasonable expectation of privacy. The U.S. Court of Appeals for the Armed Forces, while reversing in part, held that "an expectation of privacy exists in e-mail transmission made on the AOL service." Maxwell furthers the idea that a reasonable expectation of privacy exists in cyberspace.

Still, one could argue that while e-mail is more like a postal letter, surfing cyberspace is more like walking through a mall. [FN108] Thus, no reasonable expectation of privacy exists. This idea could be extended to argue that, absent a reasonable expectation of privacy, Web surfers (and shoppers) have little privacy rights. Therefore, any information collected while accessing and administering sales and use taxes on e-commerce would not violate the Web surfers' privacy rights, as they have no reasonable expectation of privacy.

The Maxwell decision was further limited by U.S. v. Monroe. [FN109] Here, the military court held that e-mail transmitted on a mailbox issued through official military channels lacked a reasonable expectation of privacy, at least with regard to superiors and the system administrator and the administrator's superiors. Maxwell and Monroe must be taken with a grain of salt, however, because they are not binding on civilians and civilian businesses. In addition, while these cases seem to recognize the right to privacy in e-mail transmissions, the particular facts of these cases could be manipulated to create arguments that either support or oppose privacy while web surfing.

The First Amendment likely also will provide some protections and limitations on privacy in cyberspace. Anyone maintaining a Web site or posting material on the Internet may be considered a "publisher." [FN110] This idea becomes especially important because the First Amendment to the U.S. Constitution protects speech, both commercial and noncommercial, and the press. [FN111] The free flow of information depicted in the First Amendment may be contrary to the idea of informational privacy. New York Times Co. v. Sullivan, [FN112] however, limits the applicability of the common law right of privacy tort when dealing with newsworthy subjects. The Privacy Protection Act of 1980 [FN113] provides further First Amendment protection by limiting the governmental seizure of publishers' work product materials. [FN114]

Finally, the Fifth Amendment protects privacy on a limited basis. [FN115] The government's ability to collect incriminating information from an individual in a variety of contexts is limited. [FN116] Thus, any action characterized as a governmental action will be similarly limited with regard to collecting information. Private papers of any kind, however, are not covered by this limitation. [FN117]

State protections. Many state constitutions provide privacy protection beyond that of the U.S. Constitution. For example, "Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have broader privacy protections." [FN118] This could be especially important if involuntary data collection violates a state constitutional right. In California, for instance, the constitutional right to privacy extends to both private and public employers. [FN119] In addition, California courts have held that the privacy provision of the California Constitution protects the inalienable right of privacy against both state and private actions. [FN120]

Furthermore, in White v. Davis [FN121] the California Supreme Court recognized that "the overbroad collection and retention of unnecessary personal information by government and business interests" fell within the privacy provision of the state's constitution. Thus, it seems as though Web sites' collecting information via cookies could violate a state constitutional right to privacy.

Major statutory protections.

The current landscape of federal privacy protection includes several statutes directed at specific industries. The following discussion briefly describes e-commerce's four most important statutes in this area. [FN122] Significantly, only the act concerned with protecting children deals in any detail or specificity with collecting, using, or disclosing personal information on the Internet. Even this forward-thinking legislation, however, protects only children from cyberspies.

Protecting children. Enacted in October 1998, the Children's Online Privacy Protection Act [FN123] is the first law to really address the collection of personal data, although, as its name implies, it applies only to information about children. The statutory regime prohibits the collection of personal information from children without parental consent. In addition, it gives parents the right to revoke consent and to access information collected about their children.

Personal information. The Privacy Act of 1974 [FN124] is the primary statute limiting the federal government's collection and use of federal agency records containing personal information. Disclosure of the data is prohibited except under certain circumstances, such as routine use, [FN125] law enforcement purposes, and for protecting an individual's health and safety. In 1988, the Computer Matching and Privacy Protection Act [FN126] amended the Privacy Act to limit computerized comparisons of two or more systems of records (e.g., records from two federal agencies, or federal and nonfederal records) in order to establish or verify an individual's eligibility for benefits or to collect delinquent debts under social benefit programs. The matching of personnel or payroll records among federal agencies or between federal and nonfederal entities also is governed by the amendment. [FN127]

Financial information. The Right to Financial Privacy Act [FN128] generally prohibits governmental authorities from accessing financial records. The Internal Revenue Service and agencies supervising banks, however, retain the ability to access certain financial information.

Electronic communication. The Electronic Communications Privacy Act of 1986 (ECPA) [FN129] limits release of information to the government by online service providers. In general, the government must have a subpoena, court order, or warrant to access an ISP's database regarding its customers. [FN130]

Conclusion

In the words of that great baseball philosopher (and player), Yogi Berra: "You've got to be careful if you don't know where you're going "cause you might not get there!" [FN131] The most significant characteristic of privacy and Internet taxation seems to be that there is no consensus on the proper actions needed to protect revenue, privacy, and the growth of the Internet. In assessing this situation, most discussion groups have not attempted to define long-term goals. The problem is that these taxation privacy issues have not been properly framed. Therefore, how can a comprehensive plan be devised when the organizations considering solutions are not aware of the specific privacy concerns? [FN132]

Most states feel that they cannot afford the loss of the tax base, but they also want to protect consumer privacy in taxing e-commerce. In addition, the states' taxing agencies may not have the legal authority to stick their hands in the out-of-state e-commerce taxationcookie jar. Congress's moratorium on Internet-specific taxes (under the Internet Tax Freedom Act) expires in October 2001. [FN133] Legislation working its way through Congress, however, would extend the moratorium until 2005 or beyond. [FN134]

The chief concern among privacy advocates is that, somehow, an avalanche of personal information would be available by enacting a taxing regime. This idea does not appear to be true. In order to administer a multijurisdictional sales and use taxation system, the address of the payor and the shipping location would be needed. In virtually every electronic transaction widely engaged in now, via, e.g., credit card or electronic transfer, this information is currently collected. An increase may result, however, in the extent of information obtained about someone using a new system of prepaid credits, such as eCash. The shipping information must currently be obtained regardless of the shipping method.

Little bits of information on people have been scattered about for years. For instance, nearly every businesses' files probably contain job, credit, and other applications containing personal information. The difference in the cyberworld is that one company could easily collect all this information and disseminate it. This idea appears particularly repugnant to the Anglo-American idea of privacy.

Therefore, the significant privacy concern relating to Internet taxation would be the matching and aggregating of

personal information. Governmental agencies, such as the IRS or the DEA, are regulated by the Computer Matching and Privacy Protection Act of 1988, which, as noted above, limits the use and matching of personal information. Thus, this fear with regard to governmental agencies is not all that well-founded. Moreover, current transactions using credit cards or electronic transfers are as traceable as any sales/use taxing information would be.

The real concern is that informational privacy would be breached by private information aggregators taking all the little bits of data existing throughout the Internet and on personal computers and compiling and distributing the information. Such a personal information picture would be too complete for many privacy advocates. In addition, using private third-parties to collect sales and use tax could create significant privacy concerns as well. For instance, these private companies would be privy to data potentially worth millions of dollars. Some device or regulatory regime would have to exist to prevent private third-party processors from collecting, aggregating, or selling their data. Otherwise, personal information of buyers could be exploited as a result of sales and use tax.

Certainly, some people feel that the Internet should not be governmentally regulated but that the market (and technology) should control. [FN135] One commentator has noted that the argument most used to support this idea is that the Internet and e-commerce have flourished because of a lack of government regulation, which would stifle innovation. But he believes the flaw in this reasoning is that the Internet's initial architecture was totally private. Therefore, it flourished because of the anonymity enjoyed by its users. This is no longer the case. While the transformation and development of technology to track users has been the defining characteristic for the last few years, the irony is that the tracking technologies developed to enable commerce to function more efficiently also made Internet regulation easier. [FN136] Therefore, the very people opposed to government regulation made the regulatory regime more feasible.

The innovative cyberworld has responded to consumer concerns about privacy. Software has been developed to ease consumers' anxieties by allowing Web surfers to create and manage their identifying data. [FN137] This complements the U.S. policy of allowing private companies to lead e-commerce. [FN138] According to many observers, the rapid advancement of technology may make legislative efforts an ineffective means of solving many e-commerce problems, including privacy issues. Technology may outpace private solutions, however. For instance, recently a Seattle-based Internet filtering software maker, N2H2, Inc., gathered marketing information on children's Web surfing patterns while in school. [FN139] Therefore, the market-regulating conduct on the Internet may not be ideal.

Problems exist with the free-market analysis concerning regulation of the Internet. For one thing, markets can fail. Not as in a stock market crash but, instead, any market condition where goods are not selling at their "market" or equilibrium price. Two significant reasons that might cause the e-commerce markets to fail and undervalue consumer privacy are (1) incomplete information, and (2) externalities. [FN140]

First, when consumers' information about market prices or service and product quality is not as accurate as the data possessed by sellers, the market will not operate efficiently. In the case of e-commerce, most consumers will not know which Web sites protect privacy. Thus, they will be unable to accurately value the cost of doing business with a particular company, either by surfing the company's Web site or by ordering goods online.

Second, the externalities of personal information privacy are not readily apparent to the consumer. Quite frankly, a Web site that maximizes the value of its consumer information by using or selling the information may be the lowest- cost provider--the value of consumers' informational privacy subsidizes some of the Web site's costs. The explicit cost of the service or goods sold via the Web site will not indicate all the implicit costs of the consumers' "selling their privacy." Therefore, consumers will purchase goods from a Web site offering the lowest price, not knowing that they are in essence selling their informational privacy to get the low price.

The misuse of private information is not a new injustice. It has been going on for as long as data has been accumulated, and still goes on by non-Internet- related companies as well. [FN141] Privacy issues are of greater concern today because it is now possible for many small organizations to amass and misuse personal information. In the past, only the government and very large organizations could compile such data, so misuses were relatively infrequent.

While U.S. laws do not elevate privacy to a human right, it is certainly a valued and treasured right--as reflected in the Constitution, case law, and statutory law. The best approach for e-commerce, and international trading in general, would be to refrain from creating a flawed, multijurisdictional taxing scheme. Nevertheless, while privacy concerns are significant to other issues, they should play no significant part in the decision to tax or not tax e-commerce. A slowing of the U.S. economy, currently in some turmoil, could prove devastating to the world's economy. Taxing e-commerce may not be in the world's best interest.

Private enterprise working together with a well-thought-out governmental regulatory regime to protect consumer privacy, along with consumer awareness, should serve to protect consumers' privacy concerns in cyberspace. This approach should keep the U.S. government from enacting an over-extensive legislative framework in the cyberspace privacy arena. Consumers must police their own privacy because no matter how much legislation is passed, some cyber pirates still will attempt to steal their personal information. [FN142]

What about e-commerce taxation?

Finally, will e-commerce be subject to sales and use taxation? Given the complexity of enforcement and collection, and questions regarding the constitutionality of such state activity, general multijurisdictional sales and use taxation probably will not occur in the near future but, as previously stated, for reasons other than privacy concerns. The complexities inherent in multistate taxation would be made even more complicated by adding sales and use taxes on e-commerce--and complexities tend to undermine a taxing system. [FN143]

One study (by Ernst & Young LLP) asserted that most of the states' income generated by e-commerce would be negated by the cost of administering the complex multijurisdictional tax system. Also, considering the various privacy laws of so many separate jurisdictions, designing the taxing system could be quite difficult. Thus, questionable significant positive cash flow because of the current economic slowdown, and difficulties associated with creating a legal framework consistent with the states' privacy laws, make it highly unlikely that a multistate sales and use tax system for e-commerce will be adopted anytime soon. A rapid increase in e-commerce revenue or decline in state and local tax revenues, however, could accelerate the time horizon for implementing sales and use taxation of e-commerce.

[FNa1]. PHILLIP W. GILLET, JR., works as a tax associate with the Law Offices of James E. Schneider, LL.M., Inc. in San Diego, California. He also is an adjunct professor of business law and accounting at San Diego City College. He thanks all those instrumental in the development of this manuscript, including Professors Matthew A. Ritter and Barry Fraser, of California Western School of Law in San Diego, for their insightful comments on previous drafts of this manuscript, and his mom for her eagle eye in proofreading. Mr. Gillet may be contacted via e-mail at pgillet@pacbell.net.

[FN1]. For purposes of this article, "e-commerce" takes on a broad meaning--more than just direct sales of goods over the Internet. The term is used to describe other, indirect income-generating activity, including (a) purchases made in-person or via telephone after visiting a Web site; (b) income generated by the sale of information obtained from data collected from Web surfers; and (c) the sale of new forms of financial instruments.

[FN2]. Nevertheless, "[t]he Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The other forms of Internet communication--e-mail, bulletin boards, newsgroups, and chat rooms--frequently have non-commercial goals." ACLU v. Reno, 929 F. Supp. 824 (DC Pa., 1996).

[FN3]. Leiner, et al., "A Brief History of the Internet," available on the Internet Society's Web site at

www.isoc.org/internet/history/brief.html.

[FN4]. "With respect to durable goods, [e-commerce] offers the opportunity to reduce dramatically the high costs associated with generating and moving transaction information on paper--estimated by some as much as 29 percent of the transaction costs in a typical cross-border purchase and sale. To the extent that international trade in digital information (including software and entertainment products such as music and video) is becoming increasingly important, electronic commerce offers virtually limitless opportunities for cost-effective commercial transactions." Sutin, "Roadblocks Stall Electronic Commerce," New York L. J., 7/13/98, page 1. Also, see "A Framework for Global Electronic Commerce," issued by the Clinton Administration, 7/1/97, available on the Internet at www.ecommerce.gov/framewrk.htm.

[FN5]. "Rulers see through spies, as cows through smell, Brahmins through scriptures, and the rest of the people through their normal eyes." Kautilya, Indian philosopher, Third Century B.C. (Quoted in Greene and Elffers, The 48 Laws of Power (Profile Books, 1998), page 104.)

[FN6]. By logging on to one Web site, www.privacy.net, a person can obtain an analysis of the type of information being transmitted about that person and their Internet connection.

[FN7]. Oberg, "Why Does Amazon.com Think It Owns My Privacy?," USA Today, 9/12/00. Recently, the Federal Trade Commission concluded that Amazon and its Alexa Internet unit likely made deceptive statements about the company's privacy policy. Amazon has now admitted that it may have "inadvertently" keep personal information in Alexa's database of Web-usage patterns. See "What's News: Business and Finance," Wall St. J., 5/30/01, page A1 (reporting FTC's conclusions); see also "FTC Says Amazon Probably Deceived on Privacy--WSJ," Reuters, 5/30/01, available on the Internet at news.findlaw.com/legalnews/s/20010530/n30552914.html.

[FN8]. "Privacy & Human Rights 2000: An International Survey of Privacy Laws and Developments--Executive Summary," available on the Internet at www.privacyinternational.org/survey/phr2000/summary.html, which also links to the full report.

[FN9]. See Kaiser Aetna v. U.S., 444 U.S. 164 (1979) (shrinking the importance of any single right by calling it one stick in the "bundle of rights").

[FN10]. See generally Quill Corp. v. North Dakota, 504 U.S. 298 (1992), which is analyzed in Eule and Richman, "Out-of-State Mail-Order Vendors Need Not Collect Use Taxes--Yet!,"2 JMT 163 (Sep/Oct 1992). See also Nolan, "Crossing the Bright Line: Evaluating Physical Presence in Quill's Shadow,"7 JMT 244 (Jan/Feb 1998).

[FN11]. Title XI of the Omnibus Consolidated and Emergency Appropriations Act of 1998, P.L. 105-277, 10/21/98. See Silverberg and Foster, "The Internet Tax Freedom Act: Will It Be a Success or a Failure?,"9 JMT 4 (July 1999). See also, Silverberg and Foster, "ACEC's Report to Congress on Electronic Commerce--Mission Accomplished?,"10 JMT 6 (August 2000).

[FN12]. Privacy Online: A Report to Congress (Federal Trade Commission, 1998), executive summary (available online at www.ftc.gov/reports/privacy3/toc.htm).

[FN13]. A broader discussion is beyond the scope of this article. Moreover, an understanding of the privacy issues

of e-commerce does not require a comprehensive summary of the taxation landscape because much of the discussion regarding other types of taxation frames the issues with reference to the concepts applicable to sales and use tax. For a detailed analysis of this area, see generally Frieden, Cybertaxation: The Taxation of E-Commerce (CCH, 2000).

[FN14]. 68 Am. Jur. 2d, Sales and Use Tax, § 1, 11 (1993).

[FN15]. J.D. Adams Manufacturing Co. v. Storen, 304 U.S. 307 (1938).

[FN16]. McLeod v. J.E. Dilworth Co., 322 U.S. 327 (1944).

[FN17]. Henneford v. Silas Mason Co., 300 U.S. 577 (1937).

[FN18]. Felt & Tarrant Manufacturing Co. v. Gallagher, 306 U.S. 62 (1939).

[FN19]. U.S. Const., amend. X, § 1.

[FN20]. Jaques, Overview of State and Local Tax Systems 1 (Arthur Andersen LLP, state and local tax education outlines, August 2000).

[FN21]. Id.

[FN22]. Id.

[FN23]. Id.

[FN24]. Id.

[FN25]. Id. See also "President Clinton and Vice President Gore Announce New Steps to Promote E-Commerce" (The White House, Office of the Press Secretary, 11/30/98), available online at www.moons.com/pres.htm (predicting that e-commerce will be hundreds of billions of dollars by 2002); "President Clinton and Vice President Gore: Putting People First in the Information Age," (The White House, Office of the Press Secretary, 11/8/99), available online at www.ed.gov/PressReleases/11-1999/wh-1108c.html (predicting e-commerce could be as much as $1.5 trillion by 2003).

[FN26]. See National Labor Relations Bd. v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1937); see also U.S. v. Darby, 312 U.S. 100 (1941); Wickard v. Filburn, 317 U.S 111 (1942).

[FN27]. Frieden, supra note 13.

[FN28]. Dreben and Werbach, "Governors: State and Federal Regulation of E-Commerce," 17 Computer Law 3

(2000), citing Ota, "States' Internet Tax Strategy," Cong. Q. Weekly (1/15/00) page 72.

[FN29]. "Industry Privacy Failures Hurting E-Commerce, Latest Surveys Show," Privacy Times (9/9/99) (citing a Jupiter Communications survey), available online at www.privacytimes.com/newwebstories/indus_priv_9_9.htm.

[FN30]. See Litan, "Law and Policy in the Age of the Internet," 50 Duke L. J. 1045 (2001), citing "Digital Economy 2000" (U.S. Dept. of Commerce, 2000), page 9.

[FN31]. See Houghton, "The Federal Legislative and NTA Tax Project Initiatives on Electronic Commerce Taxation,"8 JMT 148 (Sep/Oct 1998). See also note 11, supra.

[FN32]. See "Statement by the President [on the Internet Freedom Tax Act]" (The White House, Office of the Press Secretary, 10/8/98) (estimating 30,000 state and local tax jurisdictions), available online at cox.house.gov/chriscox/nettax/clinton.html. Other estimates place the number closer to 7,500.

[FN33]. See Quill Corp., supra note 10.

[FN34]. See, e.g., "Forms & Instructions: California 540 & 540A, 2000 Personal Income Tax Booklet," page 60, available online at www.ftb.ca.gov/forms/00_forms/00_resbk.pdf.

[FN35]. See Edwards, "Streamlined Sales Tax Project Seeks to Expand Collection of Tax by Remote Vendors," 11 JMT 6 (August 2001). See also "E- Commerce: A Threat to State and Local Tax Revenues" (AFSCME, Sept. 2000), available on the American Federation of State, County, and Municipal Employees' Web site at www.afscme.org/publications/issueb/ib0009.htm.

[FN36]. For an interesting discussion of the ironies in proposals by those favoring a regulatory-free Internet and their lack of faith in democracy, see Lessig, "Cyberspace's Constitution," a draft of a lecture given at the American Academy, Berlin, Germany, 2/10/00, available online at cyberlaw.stanford.edu/lessig/content/index.html.

[FN37]. See Caldwell, "A State Cooperative Approach to Collection of Use Taxes in Interstate Commerce," (November 1999), a proposal prepared by CommerceNet (a nonprofit e-commerce think-tank) for the ACEC (see note 11, supra), available online at www.ecommercecommission.org/document/CommerceNet122.pdf.

[FN38]. See, e.g., Loney, "Fuel Tax Agreement May Be an Example for Uniformity in Other Areas of State Taxation,"4 JMT 76 (May/Jun 1994).

[FN39]. The following brief history of the Internet provides only those relevant items necessary to effectively analyze the taxation of e-commerce. For a more detailed history, see ACLU v. Reno, supra note 2. See also Matthews, Web Publishing With Microsoft Frontpage (2d ed., Osborne McGraw-Hill, 1997); Leiner, supra note 3.

[FN40]. Matthews, supra note 39.

[FN41]. Leiner, supra note 3.

[FN42]. ACLU v. Reno, supra note 2.

[FN43]. The Web is a global "hypertext" system that uses the Internet as its transport mechanism. The system is navigated by clicking on "hyperlinks," which display other documents that also contain hyperlinks. Most Web documents are created using "hypertext markup language" (HTML), which may soon be supplanted by automated tools. Incorporating hypermedia (graphics, sound, animation, and video), the Web has become the ideal medium for publishing information on the Internet. Pfaffenberger, Webster's New World Pocket Internet Directory and Dictionary (Wempen, ed., Hungry Minds, Inc., 1997).

[FN44]. Leiner, supra note 3.

[FN45]. Id.

[FN46]. See "Statement by the President," supra note 32; see also Leiner, supra note 3.

[FN47]. Leiner, supra note 3.

[FN48]. ""Internet Privacy": An Oxymoron in Progress?," Privacy Times (2/3/00), available online at www.privacytimes.com/newwebstories/oxymoron_priv_ 2_23.htm.

[FN49]. U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F., 1996).

[FN50]. People may not be aware that their computers keep in temporary Internet files a log of Web sites visited.

[FN51]. Some surveys claim up to 85% of all Web sites collect information about their visitors.

[FN52]. The "click stream" is the "path a visitor follows through a given web site (from page to page to page)." Earles, The Internet Dictionary, available online at www.oh-no.com/define.html.

[FN53]. "In the World Wide Web..., [a cookie is] a small text file that the server writes to the user's hard disk without the user's knowledge or permission. The data in the cookies file enables one Web page to pass information to other pages, thus directly addressing a major shortcoming of the underlying Web protocol, HTTP [hypertext transfer protocol, the client-server standard for exchanging data on which the Web is based]. Many cookie applications benefit the user, for example, the shopping basket used by many "shopping malls" would not function without cookies. However, direct marketing firms are using cookies to compile information about user's browsing habits in ways that have raised grave concerns among privacy advocates. Netscape Communicator enables users to switch cookies off." Pfaffenberger, supra note 43.

[FN54]. A technical support associate at America Online (AOL), the world's largest ISP, would not directly respond to the author's inquiry regarding what click stream data AOL collects and what the company does with it.

Rather, the author was told to send the question by mail to AOL's corporate headquarters in Virginia (no e-mail address, telephone number, or contact person was provided).

[FN55]. For a detailed explanation on how to turn cookies off, see generally, e.g., The Internet for Dummies (Hungry Minds, Inc., 1999).

[FN56]. The importance of data collection to a company's bottom line cannot be underestimated because "[d]ecisions must be based on facts." Walton, Deming Management at Work (Berkley Publishing Group, 1991).

[FN57]. "The newest versions of Microsoft Internet Explorer and Netscape Navigator have extensive features for setting user profiles, managing cookies, filtering content, making use of secure digital signatures and certificates, handling encryption chores, and in general limiting the amount of information you automatically reveal about yourself on the Web." Kirchner, "Your Identity Will Be Digital," PC Magazine (6/22/99), page 143.

[FN58]. According to Amazon.com CEO Jeffrey P. Bezos: "To throttle back on investment now would be shortsighted." Id.

[FN59]. Brelsford and Wong, "Online Liability Issues: Defamation, Privacy and Negligent Publishing," 520 PLI/Pat 707 (1998).

[FN60]. See note 48, supra.

[FN61]. See Blumenfeld, "Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before the Government Steps In?," 54 Bus. Law. 349 (1998) (asserting that none of the four invasion of privacy torts provide protections broad enough to include unauthorized data collection on the Internet); see also Graham, "Note, Privacy, Computers, and the Commercial Dissemination of Personal Information," 65 Tex. L. Rev. 1395 (1987) (concluding that privacy torts do not include information privacy concerns); cf. McLaughlin, "Comment, Intrusions Upon Informational Seclusions in the Computer Age," 17 J. Marshall L. Rev. 831 (1984) (arguing intrusion upon seclusion tort should include informational privacy); see also Blackman, "A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector," 9 Santa Clara Computer & High Tech. L.J. 431 (1993) (asserting that selling or leasing of personal data constitutes a public disclosure of private facts tort).

[FN62]. See Shorter v. Retail Credit Co., 251 F. Supp. 329 (DC S.Car., 1966) (holding that a single inquiry politely conducted and quite limited in scope, when disclosed, was not an invasion of privacy.)

[FN63]. See White v. Davis, 13 Cal.3d 757, 120 Cal. Rptr. 94, 533 P.2d 222 (1975) (recognizing that "the overbroad collection and retention of unnecessary personal information by government and business interests" falls within the privacy provision of the California Constitution); see also "Crisis Control @ DoubleClick: FTC, Michigan & NY; Stock Takes Hit," Privacy Times (2/18/00), available online at www.privacytimes.com/NewWebstories/doubleclick_ priv_2_23.htm (Michigan's attorney general accused DoubleClick of violating state consumer protection laws by planting cookies on Internet users' computers without their consent; New York's attorney general also was conducting an investigation); see also McLaughlin, supra note 61; Blackman, supra note 61.

[FN64]. See "Crisis Control @ DoubleClick: FTC, Michigan & NY; Stock Takes Hit," supra note 63 (reporting

that a complaint had been filed with the Federal Trade Commission charging that DoubleClick's matching of its database of online profiles with Abacus's database of consumers' offline behavior was an unfair and deceptive trade practice).

[FN65]. See Shorter v. Retail Credit Co., supra note 62.

[FN66]. See Bradner, "Opinion: Privacy Aside, Why Chip IDs Are a Bad Idea" (CNN.com, 2/16/99), available online at www.cnn.com/TECH/computing/9902/16/chipid.idg; see also "Intel Claims PSN Will Not Be Included on New Chips," Info. Intelligence Online Newsl. (6/1/00) (available on Westlaw/Westnews, 2000 WL 9040714).

[FN67]. See "Crisis Control @ DoubleClick: FTC, Michigan & NY; Stock Takes Hit," supra note 63.

[FN68]. See generally "Clinton Remarks on Electronic Commerce Report" (7/1/97), available online at www.usis-israel.org.il/publish/econews/1997/july/eco0701c.htm. See also Dennis, "British Govt. Debates E-Commerce Guidelines" Newsbytes (10/27/97), available online at www.newsbytes.com/news/97/102350.html.

[FN69]. Note 25, supra.

[FN70]. Comparing e-commerce to the American Wild West's unregulated, unexplored, and somewhat dangerous character.

[FN71]. Hudson and McConnell, "The Internet: The Future of Finance or Fools' Gold?," 52 Consumer Fin. L.Q. Rep. 14 (1998). The "sheriff" in this instance refers to modern regulators such as the Federal Reserve Board, the Federal Trade Commission, the Federal Communications Commission, and the Justice Department.

[FN72]. "Clinton Remarks on Electronic Commerce Report," supra note 68.

[FN73]. Dreben and Werbach, supra note 28.

[FN74]. See "Remarks by Jodie Bernstein, FTC Workshop on Application of Rules and Guides to Electronic Commerce" (U.S. Fed'l Trade Comm'n, 5/14/99), available online at www.ftc.gov/opa/1999/9905/rulegu4.htm.

[FN75]. France, "Commentary: A Web Sales Tax: Not If, but When," Business Week Online (6/21/99), available at www.businessweek.com/1999/99_ 25/b3634135.htm.

[FN76]. Note 29, supra.

[FN77]. Then-Vice President Gore also felt that "[w]e are in the early stages of an information revolution ... that is bringing about dramatic changes that make knowledge the strategic resource and learning the strategic skill." "Remarks by Vice President Al Gore: Transatlantic Business Dialogue" (11/6/98), available online at clinton2.nara.gov/WH/EOP/OVP/speeches/tabd.html.

[FN78]. Technology outpacing the legal framework of privacy is certainly not a new phenomenon. By the end of the 19th Century, some commentators recognized this potential problem, noting: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual ... the right "to be left alone."" Brandeis and Warren, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890).

[FN79]. See generally Dennis, supra note 68.

[FN80]. "Green Paper on Public Sector Information in the Information Society--Public Sector Information: A Key Resource for Europe" (1/20/99), available online at europa.eu.int/ISPO/docs/policy/docs/COM(98)585/. Others cite many other reasons for the U.S.'s dominant position in e-commerce, such as "Europe's varied tax systems, high telephone costs, fewer personal computer owners and outdated encryption requirements." "European Commission Paper Seeks Reform in Electronic Commerce," 9 J. Proprietary Rts. 22 (1998).

[FN81]. Europe's interests might be served if U.S. companies were forbidden from selling through e-commerce to European Union consumers.

[FN82]. See "Forrester: Wireless Underscores Need for Privacy Overhaul," Privacy Times (3/7/01), available online at www.privacytimes.com/NewWebstories/priv_3_7_01_forrester.htm (warning American companies to aggressively confront privacy issues); "New Electronic Commerce Survey Finds Internet Poised to Become "Nation's Cash Register"," Business Wire (6/23/98), available online at www.businesswire.com/webbox/bw.062398/732483.htm (citing "[a] new poll commissioned by the Information Technology Association of America (ITTA) and conducted by Wirthlin Worldwide"). See also "GVU's 10th WWW User Survey" (October 1998), available online at www.cc.gatech.edu/gvu/user_surveys/survey- 1998-10/graphs/shopping/q182.htm (ranking security behind only "quality information," "easy ordering," and "reliability" as the most important concern when shopping or considering shopping on the Internet).

[FN83]. Hudson and McConnell, "The Internet: The Future of Finance, or Fools' Gold?," 52 Consumer Fin. L.Q. Rep. 14 (1998).

[FN84]. For example, credit card, checking account, and Social Security numbers. These two fears have remained largely unchanged for well over 30 years despite significant advances in technology. "[I]t appears that two quite different interests are being protected: freedom from physical intrusion on solitude and freedom from unwanted communication about oneself." Dixon, "The Griswold Penumbra: Constitutional Charter for an Expanded Law of Privacy?," 64 Mich. L. Rev. 197 (1965).

[FN85]. Brelsford and Wong, supra note 59.

[FN86]. "Net shoppers are nothing if not price-sensitive. In a recent study of 25,000 consumers, [University of Chicago economist Austan] Goolsbee concluded that online spending would drop by 30% or more if taxes were suddenly imposed." France, supra note 75.

[FN87]. Brandeis and Warren, supra note 78.

[FN88]. See generally Miller,"Personal Privacy in the Computer Age: The Challenge of a New Technology in an

Information Oriented Society," 67 Mich. L. Rev. 1091 (1968).

[FN89]. For an in-depth summary of U.S. Internet law, see generally Delaney and Lichstein, 505 PLI/Pat 79 (1998).

[FN90]. See Katz v. U.S., 389 U.S. 347 (1967) (stating that "the Forth Amendment cannot be translated into a general constitutional "right to privacy"" because "[t]hat Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all").

[FN91]. Id. Footnote omitted.

[FN92]. See Paul v. Davis, 424 U.S. 693 (1976) (holding that "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education" are beyond governmental intervention).

[FN93]. See Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984) (holding that information obtained during discovery may be kept private, because liberal discovery rules allow "litigants to obtain--incidentally or purposefully"-- private or irrelevant information that has not been subjected to judicial scrutiny and might never be disclosed at trial).

[FN94]. Paul v. Davis, supra note 92.

[FN95]. See National Collegiate Althletic Ass'n v. Tarkanian, 488 U.S. 179 (1988) (stating that the Constitution's protections of liberty and equal protection apply in general only to governmental actions).

[FN96]. Edmonson v. Leesville Concrete Co., Inc., 500 U.S. 614 (1991).

[FN97]. A "host" is "any computer that can function as the beginning and end point of data transfers. An Internet host has a unique address (called an IP address) and a unique domain name [or individual identifier]." Pfaffenberger, supra note 43.

[FN98]. For the state action test, see generally Lugar v. Edmondson Oil Co., Inc., 457 U.S. 922 (1982).

[FN99]. See Berman, "Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation," 71 U. Colo. L. Rev. 1263 (2000).

[FN100]. The Fourth Amendment to the U.S. Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[FN101]. See references, supra note 63.

[FN102]. 277 U.S. 438 (1928). The "intercepting [of] messages on the telephones of the conspirators" by inserting small wires into "ordinary telephone wires from residences" was high-tech at the time this case was decided. See also Radin and Wagner, "The Myth of Private Ordering: Rediscoverying Legal Realism in Cyberspace," 73 Chi. Kent L. Rev. 1295 (1998).

[FN103]. "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be left alone."" Brandeis and Warren, supra note 78.

[FN104]. Note 90, supra.

[FN105]. See Blackman, supra note 56; see also McLaughlin, supra note 56.

[FN106]. 429 U.S. 589 (1977).

[FN107]. 45 M.J. 406 (C.A.A.F., 1996), rev'g in part 42 M.J. 568 (A.F.C.C.A., 1995).

[FN108]. See Reno v. ACLU, 521 U.S. 844 (1997) (characterizing the Internet as "a sprawling mall").

[FN109]. 50 M.J. 550 (A.F.C.C.A., 1999).

[FN110]. Gindin, "Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet," 34 San Diego L. Rev. 1153 (1997).

[FN111]. The First Amendment states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." (Emphasis added.)

[FN112]. 376 U.S. 254 (1964).

[FN113]. 42 USC § 2000aa et seq.

[FN114]. For a more complete discussion of this statute, see Gindin, supra note 110.

[FN115]. The Fifth Amendment to the U.S. constitution states: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb, nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use without just compensation."

[FN116]. These contexts include police interrogations, accountant's records, and the filing of tax returns. Blumenfeld, supra note 61.

[FN117]. U.S. v. Doe, 465 U.S. 605 (1984) (O'Connor, J., concurring).

[FN118]. Gindin, supra note 110.

[FN119]. Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1st Dist., 1976) (holding that a private employer, in addition to a public employer, may violate the privacy provision of the California Constitution). "California's state constitution is the most notable because its privacy right language has been interpreted as enforceable against private parties." Blumenfeld, supra note 61 (citing Hill v. National Collegiate Athletic Ass'n, 7 Cal.4th 1, 26 Cal. Rptr. 2d 834, 865 P.2d 633 (1994)).

[FN120]. Annenberg v. Southern Cal. Dist. Council of Laborers, 38 Cal. App. 3d 637, 113 Cal. Rptr. 519 (4th Dist., 1974).

[FN121]. Note 63, supra.

[FN122]. For a more detailed look at privacy statutes, see Gindin, supra note 110.

[FN123]. 15 USC § § 6501-6506.

[FN124]. 5 USC § 552a.

[FN125]. A use consistent with the purpose for collecting the data in the first place.

[FN126]. P.L. 100-503.

[FN127]. Not covered by the amendment is the matching of records for the purposes of: law enforcement; tax collection; routine administrative programs relating to federal personnel if the match does not result in any adverse financial, personnel, disciplinary, or other adverse action against the personnel; foreign counterintelligence; producing aggregate statistical data without any personal identifiers; research projects.

[FN128]. 12 USC § 3401 et seq.

[FN129]. 18 USC § 2701 et seq.

[FN130]. See generally Wong, "Responding to Subpoenas: A Sysop's Primer for Protecting User Privacy Under the ECPA," 520 PLI/Pat 764 (1998). (Attachment 1 in Brelsford and Wong, supra note 59.) (A "sysop" is a system operator, usually a bulletin board system.)

[FN131]. Berra, "The Yogi Book" (Workman Publishing Co., 1998).

[FN132]. The Federal Trade Commission's studies into e-commerce in 1998 and 2000 wanted to protect consumer privacy; however, they did not define those privacy concerns. See "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress" (May 2000). (This report, as well as information on some other FTC actions regarding Internet privacy, are available online at www.ftc.gov/os/2000/05/index.htm#22.)

[FN133]. ITFA, § 1101(a), supra note 11. See also VandeHei and Rogers, "Election 2000: New Economy May Top Next Congress's Agenda," Wall St. J., 11/8/00, page A17.

[FN134]. See, e.g., "IPI Expert Available to Discuss Congress' Newest Action on Internet Taxes" (Institute for Policy Innovation, Media Advisory, 6/21/01), available through the IPI's home page at www.ipi.org/ipi/ipihome.nsf/home?Open.

[FN135]. See Sanders, "Firms Renew Assault on Privacy Rules," L.A. Times (3/27/01) (indicating that business leaders and members of the Bush Administration oppose pending legislation on personal privacy, especially related to Internet Commerce), available online at www.latimes.com/technology/la-000026306jul01.story. See also MacMillan, "Commerce Secretary Rejects Privacy Bills, Punts on Net Taxes," Newsbytes (3/2/00) (emphasizing then-Commerce Secretary William Daley's opposition to pending privacy legislation circulating in Congress, and stating that the Commerce Department's policy is to encourage self-regulatory privacy initiatives on the Internet), available online at www.infowar.com/class_ 1/00/class1_030200c_i.shtml.

[FN136]. See Lessig, supra note 36.

[FN137]. Many software programs have been created to protect users privacy; see, e.g., NSClean and IEClean available at http://www.privsoft.com. See also Kirchner, supra note 57 ("Novell recently announced digitalme, a software architecture to let consumers create and manage their digital identities for Internet commerce. This technology is particularly interesting because it attempts to implement the approach increasingly promoted by privacy advocates--personal control of your own identifying data. You'll be able to determine exactly which personal data you share with or sell to any Web site you visit.").

[FN138]. Id.

[FN139]. Jarvis, "Maybe This Year: Stricter Federal Internet Privacy Laws May Emerge," Marketing News (4/23/01), page 13 (available online through Westlaw/Westnews (2001 WL 6706695)).

[FN140]. "[A]n externality [exists] when a consumption or production activity has an indirect effect on other consumption or production activities that is not directly reflected in market prices." Pindyck and Rubinfield, Microeconomics (3d ed., Prentice-Hall, 1994), page 624.

[FN141]. "America's banks may face regulation over consumer privacy. Comptroller of the Currency John Hawke condemns "seamy" and "deceptive" selling of customer information to telemarketing firms. Minnesota Attorney

General Mike Hatch says U.S. Bank illegally sold Social Security, checking account, and credit card numbers to a firm that used them to sell health program memberships to bank customers. The bank denies violating any laws. [Also,] Congress may act in pending legislation that would let banks, insurers, and securities firms merge. The House Commerce Committee unexpectedly approved allowing consumers to block the sale of personal information. Privacy advocates will keep pressing for stronger protections." Ragavan, Petit, Allen, Mannix, and Terrell, "Outlook: Going After Banks That Sell Your Secrets," U.S. News & World Report (6/21/99), page 12.

[FN142]. Consider, for example, that by using any popular search engine, pirated software is readily available for downloading on the Internet, despite the illegality of such activity.

[FN143]. Gustafson, Peroni, and Pugh, Taxation of International Transactions: Materials, Text and Problems (West, 1997), page 22.

END OF DOCUMENT