

A Taxing Challenge: Maintaining Your Privacy on the Internet

By Bartlett D. Cleland

The issue of individual privacy and how government is going to protect it has been the source of much discussion at the federal, state and local levels of government. Privacy is increasingly at risk, both through electronic commerce and other modes of communication. Remote electronic application of a sales tax risks personal privacy like never before.

So what does this debate mean for consumer privacy as it relates to Internet taxation?

It means that all Americans mindful of liberty must beware of all Internet tax legislation, including legislation at the state level.

STATE LEVEL THREATS TO PRIVACY

A moratorium is currently in place on Internet taxes which are multiple or discriminatory in nature, as well as taxes on Internet access – except for those that existed prior to the moratorium. Texas is currently one of only a handful of states that taxes Internet access.

This is allowed under the “Grandfather Clause” in the current moratorium. Several states have since repealed their access tax in recognition of the need to encourage people to be on-line, and as an acknowledgment of the growing

importance of technology in the state. This moratorium is set to expire in late 2001. Between now and then Congress will be considering the many approaches it has available, and will likely pass some type of legislation. Unfortunately, the government has not been at a loss to create a means to strip an individual of the protection that privacy affords. Regardless of the federal moratorium, a great deal of discretion has been left to the individual states, including Texas.

Currently an effort is underway to collect a group of states together to configure a system to allow other governments the ability to tax local citizens. In other words, if this effort is successful, then Texans will be subjected to paying New York sales tax when making on-line purchases from companies with any presence in New York. For many reasons this scheme may fail.

Texans are uniquely placed to suffer the effects of the collection of information because of the complexity of the taxation system in Texas. Texas has, by far, the greatest number of sales and use tax jurisdictions of any state in the Union. Texas’ 1357 jurisdictions provide ample opportunity to collect even the most unimportant (from a “need to know for

Texas is currently one of only a handful of states that taxes Internet access.

purchase” standpoint) information regarding every purchase and purchaser. These jurisdictions include state, county and super-county, city, transit, economic development, and crime control district taxes. Internet tax and privacy truly impacts even the smallest political jurisdiction.

**ADVISORY COMMISSION
ON ELECTRONIC
COMMERCE**

The Advisory Commission on Electronic Commerce (ACEC), created by Congress in 1998 to study federal, state, local and international taxation and tariffs on transactions using the Internet and Internet access, managed to stumble right into a web of privacy issues. The Commission was composed of 19 members that included the governors of Utah, Virginia, and Washington, and heads of several major information technology corporations, as well as other distinguished panelists. Chaired by Virginia Governor James Gilmore, this commission was tasked with analyzing the many issues that surround electronic commerce and government and to present those recommendations to Congress. Clearly, the recommendations and subsequent legislation on the critical issues encompassing electronic commerce and tax policy will have global implications.

The result of the Commission’s work was voted on at its final meeting in Dallas in March 2000, and then reaffirmed during a conference call vote when no further compromises could be reached. The only final vote taken at the Dallas meeting regarded privacy, not taxation policy. Ironically, this was the only issue that could muster a two-thirds vote and was sent to Congress as an actual recommendation, rather than as simply a majority position.

The Commission sent the recommendation to Congress to “[e]xplore privacy issues involved in the collection and administration of taxes on e-commerce, with special attention given to the repercussions and impact that any new system of revenue collection may have upon U.S. citizens and the steps taken in systems developed to administer taxes on e-commerce to safeguard and secure personal information.”¹ This recommendation was clear – that Congress should take the time to examine the impact on privacy of any proposed e-commerce tax collection scheme.

The ACEC also recommended that Congress “[t]ake great care in the crafting of any laws pertaining to online privacy (if any such laws are necessary) to avoid policy missteps that could endanger U.S. leadership in worldwide e-commerce.”² So, the second directive is far more pointed – not only should Congress consider whether federal legislation in the arena of privacy is needed at all, but also if legislation is pursued, to understand that the privacy repercussions could be global.

The U.S. is the leader in electronic commerce. Any legislative misstep in this country will have the greatest impact on our ability to compete in world markets. Additionally, as the unquestioned technology leader, laws enacted here will likely be replicated around the world. In fact, this understanding was one of the driving forces that drove the computer software industry to fight for passage of appropriate legislation in regards to

¹ Advisory Committee on Electronic Commerce, *Report to Congress*, April 2000, p. 37. This language was submitted by Commissioner Stan Sokul and amended at the Dallas Commission meeting by Governor Locke.

² Ibid.

intellectual property during the debate on reauthorization of intellectual property laws to reflect the growing digital economy. Exceeding care must be taken or the result may be a worldwide race of governments to plunder personal information.

**PRIVATE SECTOR
VERSUS
PUBLIC SECTOR PRIVACY**

Consider for a moment that at least one division in the debate regarding privacy – particularly on-line privacy – is the fundamental difference between the government collecting information about individuals and building a database, and individuals approving the commercial use of that information.

While the government should not be provided with a means of collecting personal information under any circumstances, several reasons exist to allow a private sector concern to have access to personal information in certain situations. Perhaps the most important limitation should be a self-imposed restriction on collecting information without the individual's knowledge and consent. Providing a customer with an understanding of what information will be collected and how that information may be used would clearly provide that individual with the appropriate knowledge that personal information is being assembled. Consent could easily be obtained by informing the Web site users that information will be collected if they do not opt otherwise.

Some clear benefits flow from continuing to allow private interests to collect and use personal information. One of the popular Web business models is to allow free access to certain information on-line at no charge. These sites may be useful or entertaining to consumers, but

a cost is incurred in the development, design and maintenance of the site. One way to continue site operations is to have those costs recouped in the cost of the goods sold or the service offered.

Another, a non-sales oriented model, or a start-up model, may require that costs be recouped through the advertising on the site, as revenues may be insufficient to continue the business without the additional revenue. Regardless of which of these two models is pursued, advertising revenues may prove to be the lifeblood of the company or at least a significant source of income. In fact, the advertising revenue may be the only means through which an organization can bring its creativity and resourcefulness to the broader market.

How does any of this then relate to the use of personal information from the Web surfer? Simply put, the ability to offer prospective advertisers more tightly targeted ads through the use of personal information can greatly increase the value of the advertisements and, in turn, the level of income generated. In short, as the Internet offers consumers greater choice in regards to purchasing, concurrently the Internet offers businesses the ability to get to know their customers better. If the ability to operate a business in the free market is constrained by arbitrary legislative limitations on the type of information that a business is allowed to collect from its customers, with its customers' knowledge, then the formerly free sites will have to charge a fee for access to the information.

Additionally, to the extent that companies are given access to personal information, they can save a customer time and aggravation by offering them a more customized, efficient and satisfying on-line experience. This is

accomplished by the company displaying ads for products and services the visitor is likely to find of interest, alerting them to targeted special offers, offering alternative site directories, listing links, or providing topical chat rooms. In this way, the consumer is likely to enjoy a more relevant and interesting shopping experience.

None of this is much different from the way the world of commerce has worked throughout history. For example, the general goods stores of 100 years ago or even a clothing store today provide personalized service based on intimate customer knowledge. Would a person take offense if a thoughtful salesperson remembered a customer's name from a previous visit and greeted them accordingly? What if that same salesperson went out of their way to "set back" some of a customer's favorite product to be picked up the next time he or she visited? In some cases we could imagine that a customer may even provide a phone number so that when a limited shipment was arriving, he or she could be notified to make sure they arrived at the store in time to make a purchase. None of these scenarios seem odd or intrusive. In fact, we would characterize these experiences as helpful and perhaps as an example of the "good old days" of true customer service.

**"TRUST US. WE ARE
HERE TO PROTECT
YOUR PRIVACY..."**

Given the ACEC recommendation to Congress regarding privacy, why should anyone be concerned about the implications to personal privacy in the Internet tax debate? The answer is just below the surface of the vote in Dallas.

Privacy protections are at risk on two counts. The original vote taken in Dallas indicated a

willingness by federal, state, and local government representatives to avoid protecting the privacy of respective constituents for political gain. Governor Leavitt of Utah, Governor Locke of Washington, and Mayor Kirk of Dallas, joined by the representatives of the Treasury Department, Commerce Department and the U.S. Trade Representative, each originally abstained from the vote to protect consumer privacy. Later, the two governors and the mayor returned to ask if they could reopen the vote so that they could reverse their position, while the federal representatives stood firmly against supporting consumer privacy. The lesson learned from this demonstration is fairly simple: when put to the test, the initial position of many who represent various levels of government in elected office appears to be to protect a political position at any cost, even if that cost erodes individual liberty.

Even more onerous is the position the federal government representatives held. Their position, originating from a National Governor's Association (NGA) proposal, called for a system that would track everything about an individual, including where a purchase took place, what was purchased, who purchased the item, the purchaser's address, and payment information.

To make this system work the NGA proposed a collection scheme with a "Trusted Third Party (TTP)" designated to collect all of the consumer's information. The proposed TTP would be the agent in effecting a shift in sales tax administration away from the states directly, a concept called tax farming. Under this model, the participating states would "farm out" work to a separate entity with responsibility for calculating, collecting, reporting, and remitting the appropriate amount of sales tax back to the states. In effect,

the TTP would develop a national database of personal purchasing information as a national clearinghouse and tracking entity for all purchases.

After the original plan was sharply criticized, the NGA replaced it with a somewhat reworded version. However, the fundamentals were the same and rather than promoting the use of the TTP, the language was simply changed to use a "payment processing system" and "qualified service provider." These entities would still gather all of the personal information on all purchases. In other words, the NGA proposal has not changed and still dramatically destroys consumer privacy.

The original and the "new" NGA plan includes a fig leaf regarding privacy concerns. The governors indicate that the plan will "...ensure that personal information is not unnecessarily gathered and is not improperly used by persons acting on behalf of the states." Unfortunately, the governors clearly intend that personal information be gathered and that the only protections are after the fact, that is, after the information is improperly used. Accordingly, the only effort to protect privacy is to protect a person from someone using his or her personally identifying information for unrelated purposes. Under this regime, the state and local governments will develop a national database of personally identifying information to track all purchases so that they may levy a tax.

In short, though the NGA has removed the title of TTP from its plan, the TTP concept persists. Avoiding the detail does not make the concept any more palatable. The NGA will subsequently have to put more detail into its plan. This detail will again clearly show that the intention is to collect personal information from all consumers for the "privilege" of participating in the stream of commerce. As in many

situations, an idea may sound good until the details are examined. In this case, as the NGA plan moved from concept to reality, the implications for personal privacy were enormous.

The guiding thought for the government proposal seems to be that everyone should trust a central collection point operated by the government to do a "good enough" job of protecting individual and organizational privacy. Beyond the terrifying constitutional ramifications, there appears to be a clear lack of understanding by the government entities that the information it proposes to collect and retain far exceeds that which is currently collected.

At the federal level, the Clinton Administration has been promoting a legislative means to allow the federal government to ration privacy. At the same time, several federal agencies, including the Federal Bureau of Investigation (FBI), seek to have full access to all electronic communication without a person's knowledge and without due process protections. One such example is a system designed to run on an airline's computer system that would search through a passenger's proprietary information and randomly select passengers to pull aside to search through luggage and person, a system being championed by Vice-President Gore.³ Also, not long ago the Federal Trade Commission (FTC) was charged with moving too swiftly to impose new regulations on the Internet without considering how those government regulations could harm small Web sites.⁴ Of course, one of the most

³ *You? A Terrorist? Yes!*, Wired.com News, 20 April 1999.

⁴ *FTC Critics: Go Slow on Privacy*, Wired.com News, 11 June 1999.

harmful proposals was from the FTC to form a “special” e-commerce enforcement bureau unit within the agency to regulate the increasing level of electronic commerce.

The most likely outcome in the Internet tax debate will be a vote to extend the moratorium. This issue may or may not be tied to requirements that the individual states simplify their sales tax structure. Unfortunately, the focus will likely center on taxation, not on protecting the consumer from a massive invasion of privacy. This issue may force the consideration of consumer privacy on-line, as privacy is a major concern in any electronic taxation process. It is likely that several independent pieces of the Commission’s recommendation will start traveling through Congress rather than through a larger and more comprehensive package. For example, a bill regarding access taxes would be introduced independent of legislation regarding a moratorium extension.

A monstrous and invasive information collection scheme will likely not be passed in this Congress, but not due to lack of desire from our nation’s state and local governments. Governments will continue to sing the siren song of greater protection of your privacy – and assert that the bureaucracy can protect personal information better than individuals can for themselves. However, with the misguided concept of a central database through which all consumers and purchases must pass, individual liberty and the digital economy are both highly threatened.

Bartlett D. Cleland (bcleland@ipi.org) is the Director of the Center for Technology Freedom at the Institute for Policy Innovation (IPI). He was formerly Technology and Policy Counsel for Americans for Tax Reform, and earlier, counsel to U.S. Senator John Ashcroft.