

**Subj:** Online Privacy: Perspectives of AllAdvantage.com  
**From:** Ray Everett-Church, CPO, AllAdvantage.com, c/o Michael Moore, 415-391-2994, michael\_moore@bhimpact.com  
**To:** Internet Caucus Advisory Committee

**Privacy from Whom (Government Intrusion vs. Corporate Intrusion)  
- Privacy from Corporations (e.g. Marketer solicitations)**

There is an alternative emerging to secret online profiling. It is a new consumer-oriented model: the Infomediary. Infomediaries work as a personal agent on behalf of consumers to help them take control over the profiling process. Infomediaries operate on the assumption that personal information is the property of the individual described, so individuals should have the means to share in the value created by their BM\_1\_personal information if they so choose.

One such Internet infomediary is AllAdvantage.com. Its implementation of the infomediary concept recognizes the valuable nature of personal data and acts as a trusted agent for consumers, providing both the opportunity and means for its members to monetize their own online profiles without compromising the privacy of the data. AllAdvantage.com uses its Viewbar(tm) technology to build a profile of an individual member's online viewing and purchasing habits. Collecting these profiles and aggregating them with those of other members, AllAdvantage.com negotiates with marketers and vendors to the benefit of members.

As a necessary element of its business, infomediaries such as AllAdvantage.com build relationships with consumers based on fair information principles of explicit notice, limitations on collection and use of consumer data, consumer access and redress, and clear and unambiguous consent. For example, AllAdvantage.com explicitly discloses to members, even before they join, what information will be collected about them to build their unique profile, how the individual may stop the collection of information, and how that information will be used once collected. Finally, members are allowed to terminate the relationship at any time, and they may request that their personally identifiable information be blocked from further use.

**Subj:** Online Privacy: Perspectives of Institute for Policy Innovation  
**From:** Bartlett Cleland, 972-874-5139, bcleland@ipi.org  
**To:** Internet Caucus Advisory Committee

## **Trust Me: the Internet tax debate and your privacy**

By Bartlett Cleland

No one should be surprised that so many Americans are concerned about their individual safety and privacy, particularly where the government is concerned. The news in the last several weeks has certainly provided much reason for real worry. Whether the door busting tactics of the Immigration and Naturalization Service in a dark of night raid in Miami, to the continued push by the FBI on Capitol Hill to have unfettered access to your email, to the ECHELON system that accumulates and tracks all electronic communication in this country for NSA purposes -- certainly the assault on our privacy is in full swing.

### ***The Advisory Commission on Electronic Commerce***

Privacy implications are cropping up in less obvious places than raids and overt spying by the U.S. government on the American public. One of these arenas was the Advisory Commission on Electronic Commerce. The Advisory Commission on Electronic Commerce (ACEC) was created by Congress in 1998 to study federal, state, local and international taxation and tariffs on transactions using the Internet and Internet access.

The Commission was composed of 19 members that included the governors of Utah, Virginia, and Washington, and heads of several major information technology corporations among others. Virginia Governor James Gilmore chaired the commission. This commission was tasked with analyzing the many issues that surround electronic commerce and government and to present those recommendations to Congress. Without a doubt the recommendations on the critical issues of electronic commerce and tax policy will have global implications as they find their way into legislation.

The end result of the Commission's work was voted on once at the final meeting in Dallas, and then reaffirmed during a conference call vote when no further compromises could be reached. The only vote to be made final at the Dallas meeting was in regards to privacy, not taxation policy. Ironically, this was the only issue that would achieve a two-thirds vote and later sent to Congress as an actual recommendation, rather than as 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."<sup>1</sup> The recommendation here was clear – that Congress should take the time to examine the impact on privacy of any tax collection scheme that is proposed.

---

<sup>1</sup> 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.

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.”<sup>2</sup> So, the second directive is far more pointed – not only should Congress consider whether federal legislative in the arena of privacy is needed at all, but if they move forward with legislation to understand that the repercussions could be global.

The U.S. is the leader in electronic commerce so a mistake in this country will have the greatest impact on our own ability to compete. Additionally, since the United States is a leader in technology that the laws enacted here will be replicated around the world. In fact, this understanding was one of the driving forces that drove the software industry to fight for passage of appropriate legislation in regards to intellectual property during the debate on updating intellectual property laws to reflect the growing digital economy. So, exceeding care must be taken or the result a worldwide race of governments to plunder your 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 you and building a database, and when a person approves a commercial use of their information.

While the government should not be provided with a means of collecting your personal information under any circumstances, several reasons may exist to have a private sector concern know your 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 approval. Providing a customer with an understanding of what information will be collected and how that information may be used would clearly provide a person with the appropriate knowledge. Approval could easily be obtained by informing the Web site user that information will be collected if they do not opt otherwise.

Some clear benefits could flow from continuing to allow private interests to collect and use information about you. One of the popular Web business models is to allow free access to certain information on-line for free. These sites may be useful to consumers or even entertaining, but a cost is incurred in the development, design and updating of the site. One way to continue site operations are to have those costs recouped in the cost of the goods sold or the service offered. Another, non-sales oriented model, or a start-up model, may require that the costs are recouped through the advertising on the site as revenues are insufficient to continue the business without the additional revenue. Regardless of which of these two models are pursued, advertising revenues may prove to be the lifeblood of the company or at least a significant source of income. That is to say that the advertising revenue may be the only means with which an organization can bring its creativity and resourcefulness to the broader market.

---

<sup>2</sup> Ibid.

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. That is to say that as the Internet offers consumers greater choice in regards to purchasing, and in turn 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 customer's knowledge, then the formerly free sites will have to charge a fee to access of 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 efficient and satisfying online 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, lists of links, or even 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 than the way the world of commerce has worked forever. Take for example, the general goods stores of 100 years ago or even a clothing store today. 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 particular customer's favorite products so that they could pick it up the next time they visited? In some cases we could imagine that customer may even provide a phone number so that when a limited shipment was coming in they 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 them 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..."**

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

On two accounts privacy protections are at risk. The original vote taken in Dallas indicated a real willingness by the federal, as well as the state and local government representatives avoid protecting the privacy of its constituents for political gain. Governor Leavitt of Utah, Governor Locke of Washington, and Mayor Kirk of Dallas, joined with the representatives of the Treasury Department, Commerce Department and the U.S. Trade Representative, and all 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 change 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 those who represent any level of government seems to be to protect a political position at any cost – even if that cost is the sacrifice of the rights of their own constituents.

## Online Privacy Part 2: Privacy From Whom (Government Intrusion vs. Corporate Intrusion)?

---

Even more frightening -- the position the government representatives held is consistent with a proposal that they have circulated. The original proposal circulated by the National Governor's Association (NGA) called for a system that would track everything about an individual including where a purchase took place, what was purchased, who purchased the item, where they live, and payment information.

To make this system work the NGA proposed a collection scheme with a "trusted third party" designated to collect all of a consumer's information. In addition, each person would be assigned a "geo-code" so that the central collection authority, the "trusted third party" could track the purchases of the individual. In other words, you would need to have your "geo-code" to be able to purchase items either on-line or through a catalog, and eventually even brick-and-mortar store purchases. The long-term goals that are claimed is a simplified system for taxation and a "completely unified" system in the states, which would end the concept of competition among the states, and in other words, the plan would end federalism.

The proposed "Trusted Third Party" (TTP) would be the agent of allowing a shift in sales tax administration away from the states directly, a concept called tax farming. That is to say, that the participating states would "farm out" its work to a separate entity with responsibility for calculating, collecting, reporting, and remitting the appropriate amount of tax back to the states. In effect, the TTP would develop a national database of personal purchasing information as a national clearinghouse and tracking device for all purchases.

The "geo-code" concept was developed to pinpoint the rate of tax to be added to a particular purchase. As taxes do not follow zip code or congressional district lines a new system would have to be developed. This "geo-code" would be used to determine a tax rate based on residence. The Internet makes difficult the proposition of taxing a transaction based on geographical limitations. A very simple example demonstrates the difficulty. A tourist from Oregon could be in Texas with a laptop computer and a wireless modem, making a purchase on a Web site hosted on a computer in Florida, from a company whose headquarters are in Maine, with warehouses in Illinois, and that tourist could choose to have the purchase sent to their second home in Colorado. Where did the transaction take place?

This new "geo-code" would determine that the tax should be paid in Oregon, so that no one could buy or sell unless they had the "geo-code," which is the number associated with where they live.

After the original plan was sharply criticized on a number of grounds the NGA replaced it with a somewhat reworded version. The fundamentals are the same and instead of the use of the TTP the language simply changed to using a "payment processing system" and "qualified service providers." These entities would still perform all of the personal information collecting and "geo-code" application on all purchases. In other words, the NGA proposal has not changed, and dramatically destroys consumer privacy at many levels.

The original and "new" NGA plan both include some effort to acknowledge 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 will be gathered and that the only protections are after the fact, that is, after the information is

improperly used. So, the only effort to protect privacy is really to protect a person from someone using their personally identifying information for their own 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.

*The bottom line is that even though the NGA has removed the tile of TTP from their plan, in fact the TTP concept still exists. Avoiding the detail does not make the scheme any more palatable. At some point the NGA will have to put more detail back into their 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 your privacy. What seems to be missing is any understanding by the government entities that the information they want to collect and hold is far more than would be collected in any way now.*

*What to watch for...*

*So what does this debate mean for consumer privacy as it relates to Internet taxation? It means – watch out!*

*Currently a moratorium on new taxes, multiple or discriminatory sales taxes, as well as taxes on access to the Internet is in place. This moratorium is set to expire in October of 2001. Between now and then Congress will be considering the many approaches it has available, and will very likely act in a legislative move. Unfortunately, the government has not been at a loss to create a means to strip an individual of the protection that privacy affords.*

*Over the last several months the Administration has been pushing for a legislative means to put the federal government in charge of your privacy. At the same time several federal agencies including the FBI seek to have full access to all electronic communication without a person's knowledge and without due process protections. Just one example is a system designed to run on an airline's computer system which would search through a passenger's proprietary information and randomly select passengers to pull aside to search through their luggage and person – this system is being championed by Vice-President Gore. Also, not long ago the FTC was charged with moving too swiftly to impose new regulations on the Internet without even considering how those government regulations could harm small Web sites. Of course, one of the most harmful proposals was from the FTC to form a "special" e-commerce enforcement bureau unit within the FTC 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, and that may or may not be tied to requirements that the individual states simplify*

---

<sup>3</sup> *You? A Terrorist? Yes!*, Wired.com, 20 April 1999.

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

*the tax structure. The problem is that the focus will likely only be 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 scheme. Likely, several independent pieces of the Commission's recommendation will start travelling through Congress instead of in one large package. So, for example, a bill regarding access taxes would be introduced independent of legislation regarding a moratorium extension.*

*A large information collecting scheme will likely not be passed in this Congress, but not do to lack of desire from the nation's state and local governments. Governments will continue to sing the siren song of greater protection of your privacy – that they can protect your personal information better than you can protect it yourself. However, with their notion of a central database through which all consumers and purchases must pass, consumers and the digital economy are both highly threatened.*

Bartlett Cleland 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 Senator John Ashcroft. Please email to [BCleland@IPI.org](mailto:BCleland@IPI.org)