Proposal on Taxation of Electronic Commerce
to the
US Advisory Commission on Electronic Commerce
November 1999

Jon M. Peha[1]

A system for collecting taxes must be technically feasible, efficient, and cost-effective. This includes the procedures for determining tax rates, collecting taxes, transferring funds to the appropriate government authority, and proving to an auditor that taxes were paid. This proposal reconciles some important policy objectives with current and emerging technology.

Highlights of Recommendations

- Electronic commerce vendors should be required to keep verifiable records for tax audits. Procedures should be established for creating verifiable records. These procedures would involve accredited third parties: *electronic notaries* and *verifiers*.
- A system of voluntary accreditation for *electronic notaries* should be established. Accredited notaries should meet specific financial and technical criteria; they should be capable of establishing when records were notarized and insuring that records cannot be altered subsequently without significant risk of detection. Notaries must also be able to assemble all records submitted for notarization by a given vendor within a specified time period.
- A system of voluntary accreditation for *verifiers* should be established. Accredited verifiers should meet specific financial and technical criteria; they should be capable of insuring that customer identities and credentials are accurate, and that items that have received an electronic signature cannot be altered subsequently without significant risk of detection.
- Government should oversee accredited notaries and verifiers to insure trustworthy operation.
- Government should advertise a list of accredited notaries and verifiers.
- Vendors should be required to collect taxes on all sales that are taxed, regardless of the location of the vendor or the buyer. The sales tax should be based on the official location of the buyer.
- When an information product is purchased via electronic commerce, the official location of the buyer should be based on static characteristics of the buyer, like the buyer's tax home.
- States should simplify the process of determining tax rates on sales to out-of-state customers. For example, they could harmonize rates, or define a set of product categories (like "food") that are common nationwide. In any given jurisdiction, all products from the same category would be taxed at the same rate, although the rate for that category could differ from one jurisdiction to another.
- State-wide or regional clearinghouses should accept taxes collected by vendors, and distribute those funds to the appropriate local authorities.

[1] Professor of electrical engineering and public policy, Carnegie Mellon University, Dept. of ECE, Pittsburgh, PA 15213-3890, peha@ece.cmu.edu, (412) 268-7126, http://www.ece.cmu.edu/~peha

Guiding Principles

- A consumer should pay the same tax on an item that is purchased through electronic commerce as she would pay on an item purchased at the local store. Imposing higher taxes on electronic commerce would discourage growth of this vital new marketplace. Imposing higher taxes on traditional commerce would penalize consumers who cannot afford a computer and Internet access, thereby exacerbating the digital divide.
- A consumer should pay the same tax rate on information that is contained in a physical package (such as a compact disk, a book, or a videotape) as she would pay on information that is not. To do otherwise would be to unfairly favor one industry over another, and it would decrease the efficiency of the market.
- Vendors should collect sales tax in electronic commerce transactions, just as they do in traditional commerce.
- Transactions should produce a trustworthy audit trail so that tax evasion can be detected and therefore deterred. Any attempt to forge, delete, or retroactively alter records must face significant risk of detection, even if buyer, seller and/or third parties involved in the transaction cooperate in the attempt.
- Neither buyer nor seller should be required to sacrifice any privacy to the other party, or to third parties such as credit card companies. Undermining privacy would hinder growth of electronic commerce.

Rationale for Recommendations

The need for auditability

Taxes cannot be enforced without auditable records that are trustworthy – even if buyer and seller might try to alter those records. Traditional commerce generates paper trails that are difficult to alter or forge, like cash register logs, signed bills of sale, and shipping records. Electronic commerce often produces only electronic records which are easily changed without risk of detection.

The problem is worse when the transaction takes place entirely over a network as occurs with an information product. Sale of information such as text, music, videos, and software over the Internet will become increasingly common. Such transactions create two problems for tax auditors. First, transactions leave no physical evidence behind. Second, unlike a physical product, information can be sold many times. Thus, revenue figures cannot be corroborated by examining inventory. Auditors must depend entirely on transaction records. If transaction records can be changed without risk of detection, any policy that requires such records for enforcement is doomed.

Records must be generated for each transaction. Any attempt to forge, destroy, or retroactively alter records must face significant risk of detection. Records stored electronically can be changed without detection. If a vendor and customer agree to such a change, or if the customer's records will be unavailable (as is often the case), then vendors can alter records with impunity. A third party is necessary if transaction records are to be trustworthy. This might be a credit-card company. But how does an auditor know the third party’s records will be correct, complete, and available? Today, it is impossible, making problems inevitable.

Moreover, transaction records must go to third parties without undermining privacy. Today, many electronic commerce customers and merchants entirely surrender their privacy to a credit-card company, and to each other. It is no surprise that Internet users routinely cite privacy concerns as their primary reason for not engaging in more electronic commerce. Parties should not be forced to reveal anything beyond the credentials necessary for that particular transaction, which need not include identity. Even that information should be unavailable to everyone outside the transaction, except for authorized auditors. It should even be impossible to determine whether a particular person has engaged in any transactions at all.

An effective system

There is a practical system that solves many of these problems at little cost to vendors, and no cost to consumers. (The system also helps to prevent fraud and illegal sales [1].) Conceptually, it works as follows: All parties create a record containing the specifics of a transaction. All parties sign it. A party that is subject to audits then has its copy notarized. This system will be summarized here. (See [2] for more technical details.)

To enable a true audit, outside entities must be involved in recording the transaction. This system includes *verifiers* and *notaries*. Verifiers check the identity of all parties and vouch for credentials. Notaries oversee every transaction record, establishing a time and date and insuring that any subsequent modifications are detectable.

Separating verifier and notary functions is crucial. A verifier knows the true identity of some customers. Notaries know whether that verifier's unidentified customer is engaged in transactions, and perhaps some information about those transactions. If an organization (like a credit-card company) served as both verifier and notary, it could know that a given person is participating in specific transactions, thereby undermining that person's privacy.

Any person or company that wants an audit trail must first register with one or more verifiers. To register, this person tells the verifier her public key, but not her secret key. She has the option of providing additional information, which she may designate either public or private. Public information can be used as credentials during transactions. Private information may later be accessed by authorized auditors. The verifier is responsible for checking the veracity of all customer information, public and private.

For example, one individual might provide her name and social security number as private information, and her US citizenship as public information. Her nationality, public key, and account number are publicly displayed on the verifier's Web site. Auditors can check her identity if necessary. Vendors know only her verifier account number and citizenship, allowing her to anonymously purchase American software that has export restrictions.

This individual might also register with a second verifier. This time, she declares as public information that she is a software retailer, so she can avoid certain sales taxes. She keeps her nationality confidential. Because she has two verifier accounts, no one can determine that she is both a software retailer and a US citizen.

For each verifier account, a relationship is established with one or more notaries. A government agency is informed of all verifier accounts and relationships with notaries. Then, electronic commerce transactions can begin.

In a transaction, all parties create a description of the relevant details using a standardized format which contains enough information to determine the tax amount, the tax jurisdiction, and the tax period. For a software purchase, the description might include the software title, warranty, price, date, time, and the official locations of buyer and seller. A transaction record would consist of this description, plus the electronic signature and verifier account of each party. The record would be equivalent to a signed bill of sale, and would prove that all parties agreed.

Entities that are not subject to audits, including most consumers, would be largely unaffected by this system. Each party that requires an audit trail would submit its copy of the transaction record to an associated notary. This makes it possible to later audit one party without viewing the records of the others. It is possible to "hash" the record so the notary cannot understand, which protects the privacy of all parties. A party submitting a record must also provide verifiable proof of identity, probably using a verifier account number and an electronic signature, or biometric data. This allows the notary to later assemble all records submitted by a given vendor, so auditors can catch a vendor that fails to report some transactions. The notary adds a timestamp and processes the record. Once a record is processed, subsequent changes are detectable by an auditor, even if all parties to the transaction and the notary cooperate in the falsification [2].

The notary also creates a receipt. Anyone with a notarized record and the associated receipt can verify who had the record notarized and when, and can determine that no information has subsequently been altered.

Several notaries and certificate authorities currently provide some necessary verifier and notary functions, but not all. For example, there are notaries that establish the date of a transaction, but none can produce a list of all transactions notarized for a given vendor, which is essential. There is little incentive for entrepreneurs to offer such services, given that a notary’s output is rarely called for, or recognized, under today's laws.

If government leads, industry will build

Trustworthy commercial verifiers and notaries are needed. A government agency or government contractor could provide the services, but private companies would be more efficient at adapting to rapid changes in technology and business conditions. Commercial competition would also protect privacy because it allows customers to spread records of their transactions among multiple independent entities. Like notary publics, banks, and bail bondsmen, verifiers and notaries would be private commercial entities that play a crucial role in the nation's financial infrastructure and its law enforcement.

How would anyone know that services provided by a private company are trustworthy? Government should support voluntary accreditation of verifiers and notaries. Only accredited firms could be used when generating records to comply with tax laws or to interact with government agencies. Individuals and private companies would still be free to use unaccredited notaries and verifiers in private transactions.

To obtain accreditation, a verifier or notary would demonstrate that its technology has certain critical features. A notary, for example, would show that any attempt by the notary or its customers to alter or delete a notarized record would be detectable. The system must also be secure and dependable, so the chances of lost data are remote. The specific underlying technology used to achieve this is irrelevant. Accredited firms must also be financially secure and well-insured against error or bankruptcy. The insurer guarantees that even if a notary or verifier business fails, the information it holds will be maintained for a certain number of years. The insurer therefore has incentive to provide effective oversight.

Government oversight is needed to make this system work. To insure that records have not been altered, notaries and verifiers should be subject to limited federal oversight, including the possibility of random audits. Such oversight is typical for commercial enterprises that are accredited by government. Some government agency or agencies must also keep track of the verifier and notary accounts held by every electronic vendor. This prevents a vendor from keeping multiple sets of electronic records, and deciding which to reveal when audited.

Collecting taxes on out-of-state sales

To meet the requirement that a customer pay the same tax for an item purchased via electronic commerce as an item purchased in a local store, the tax for both must depend on the location of the buyer - regardless of the location of the vendor. Moreover, the tax must actually be collected on electronic commerce. This means that an out-of-state vendor may be required to collect this tax, even if this vendor has no physical presence in the buyer's state. (The objectives of fairness and economic efficiency would be achieved whether the collected tax goes to the state where the vendor is located, the state where the buyer is located, or the federal government.)

Steps must be taken to minimize the overhead associated with tax collection. With 30,000 tax jurisdictions, it is difficult for a vendor to know the tax rate on every item sold. Different jurisdictions have different rates. Moreover, there can be different rates for specific product categories like food or newspapers, and the definitions of "food" and "newspaper" also vary from one jurisdiction to another.

It would help to harmonize tax rates across jurisdictions, at least within state boundaries. This might be difficult to achieve, as it can limit a local authority's ability to raise tax revenues. Many of the practical benefits of harmonization can be achieved with little loss of local autonomy by simply harmonizing product categories. For example, all food products might be taxed at 2% in one jurisdiction and at 5% in another jurisdiction, but a product that is considered food in one jurisdiction is considered food in all jurisdictions. Tax rate would then depend only on a product's category, which is well-defined nationwide, and tax jurisdiction, which would be determined from the official address by software.

Vendors also need a simple means of transferring the taxes they collect. Each state or collection of states could create a clearinghouse that accepts funds from out-of-state vendors and distributes them to the appropriate local authority.

Location of the buyer

When a physical product is mailed to a buyer, it is not unreasonable to use mailing address as the buyer's official address. However, when an information product (like software or digitized music) is transmitted over the network, there is no mailing address. An electronic commerce vendor cannot always know where a buyer is located. Indeed, some systems are designed specifically to obscure that information, as a convenience to users [3]. Thus, vendors should not be held accountable if buyers lie about their location at the time of the purchase.

By using verifiers, vendors do have the ability to check static information about the buyer, such as the address that an individual declares when filing income tax returns or registering to vote. Thus, it is better to establish the official location of the buyer using static information rather than the location of the buyer at the time of the purchase.

State and federal roles

Government agencies have a variety of tasks to perform. Verifiers and notaries must be accredited. Vendors must register with a government agency. Random audits must insure that registered vendors collect taxes due to any state. It would be most efficient for a single agency to take responsibility for some of these tasks - probably a federal agency. This raises complex issues of federalism. There are many viable approaches to establishing a useful federal role. These include federal legislation with some state preemption, federal legislation that allows states to opt in, expansion of existing federal programs such as unemployment tax [4], and establishment of uniform state laws. States have incentive to cooperate in promoting uniformity to insure that states tax laws can be enforced, and to prevent the expense of duplicating oversight responsibilities unnecessarily. The tradeoffs among these and other options are beyond the scope of this proposal.

References

[1] Jon M. Peha, "Making the Internet Fit for Commerce: policies to enforce tax laws, protect privacy, deter fraud, and prevent illegal sales," *Issues in Science and Technology,* National Academy Press, Winter 2000.
[2] Jon M. Peha, "Making Electronic Transactions Auditable and Private," *Proceedings of the Internet Society's INET-99*, June 1999.
[3] Jon M. Peha and Robert P. Strauss, "A Primer on Changing Information Technology and the Fisc," *National Tax Journal*, Vol. L, No. 3, Sept. 1997, pp. 608-21.
[4] Robert P. Strauss, "Further Thoughts on State and Local Taxation of Telecommunications and Electronic Commerce."

References are available at http://www.ece.cmu.edu/~peha/ecommerce.html

CRITERIA FOR EVALUATION OF ALTERNATIVE PROPOSALS

1. HOW DOES THIS PROPOSAL FUNDAMENTALLY SIMPLIFY THE EXISTING SYSTEM OF SALES TAX COLLECTION?

- Regional or state-wide clearinghouses would be established for distribution of taxes.
- For sale of information products, the buyer's location would be based on static information such as tax home rather than location at the instant of the sale.
- A definition of product categories could be standardized nationwide.

2. HOW DOES THIS PROPOSAL DEFINE, DISTINGUISH, AND PROPOSE TO TAX INFORMATION, DIGITAL GOODS, AND SERVICES PROVIDED ELECTRONICALLY OVER THE INTERNET?

Information and digital goods would be taxed at the same rates as tangible goods.

3. HOW DOES THIS PROPOSAL PROTECT AGAINST ONEROUS AND/OR MULTIPLE AUDITS?

Because vendors are required to use accredited verifiers and notaries in the formation of records, those records are trustworthy. Auditors can therefore focus more on the records, and less on the system that produces them, making audits far less onerous. This also makes audits far more effective, so the same level of deterrence for tax evasion can be achieved with fewer audits.

4. DOES THIS PROPOSAL IMPOSE ANY TAXES ON INTERNET ACCESS OR NEW TAXES ON INTERNET SALES?

No. Taxes on Internet sales should be the same as taxes on other sales.

5. DOES THIS PROPOSAL LEAVE THE NET TAX BURDEN ON CONSUMERS UNCHANGED?

This proposal does not change the tax obligation on consumers. It merely allows existing taxes to be collected, and tax evasion detected.

6. DOES THE PROPOSAL IMPOSE ANY TAX, LICENSING OR REPORTING REQUIREMENT, COLLECTION OBLIGATION OR OTHER OBLIGATION OR FEE ON PARTIES OTHER THAN THOSE WITH A PHYSICAL PRESENCE IN A PARTICULAR STATE OR POLITICAL SUBDIVISION?

Vendors would be required to collect sales tax, regardless of whether they have a physical presence in the buyer's state. This proposal does not specifically address whether the taxes would go to the buyer's state or the seller's state.

7. WHAT FEATURES OF THE PROPOSAL WILL IMPACT THE REVENUE BASE OF FEDERAL, STATE, AND LOCAL GOVERNMENTS?

Revenues will increase, because existing taxes on interstate and intrastate electronic commerce will be collected, and tax evasion will be deterred.

8. DOES THIS PROPOSAL REMOVE THE FINANCIAL, LOGISTICAL, AND ADMINISTRATIVE COMPLIANCE BURDENS OF SALES AND USE TAX COLLECTIONS FROM SELLERS? DOES THE PROPOSAL INCLUDE ANY SPECIAL PROVISIONS WITH RESPECT TO SMALL, MEDIUM-SIZED, OR START-UP BUSINESSES?

The proposal would allow collection of sales tax on electronic commerce with limited new compliance requirements. The proposal does not differentiate small and large businesses.

9. DOES THE PROPOSAL TREAT PURCHASERS OF LIKE PRODUCTS OR SERVICES IN AS LIKE A MANNER AS POSSIBLE THROUGH THE IMPLEMENTATION OF A POLICY OR SYSTEM THAT DOES NOT DISCRIMINATE ON THE BASIS OF HOW PEOPLE BUY?

Yes. The proposal would make it possible to eliminate discrimination between products purchased via electronic commerce and traditional commerce, and discrimination between tangible products and information products.

10. DOES THE PROPOSAL DISCRIMINATE AGAINST OUT-OF-STATE OR REMOTE VENDORS OR AMONG DIFFERENT CATEGORIES OF SUCH VENDORS?

No. The proposal would eliminate discrimination, causing out-of-state vendors to collect taxes at rates that are identical to in-state vendors in sales to a given consumer.

11. HOW DOES THIS PROPOSAL AFFECT U.S. GLOBAL COMPETITIVENESS AND THE ABILITY OF U.S. BUSINESSES TO COMPETE IN A GLOBAL MARKETPLACE?

The proposal specifically addresses domestic taxation.

12. CAN THIS PROPOSAL BE SCALED TO THE INTERNATIONAL LEVEL?

The proposal could be the first step to allow international electronic commerce without onerous overhead associated with tax collection. This would greatly benefit electronic commerce vendors in the US, and elsewhere.

13. HOW DOES THIS PROPOSAL CONFORM TO INTERNATIONAL TAX SYSTEMS, INCLUDING THOSE THAT ARE BASED ON SOURCE RATHER THAN DESTINATION? IS THIS PROPOSAL HARMONIZED WITH THE TAX SYSTEMS OF AMERICA'S TRADING PARTNERS?

This proposal would establish domestic sales tax at a rate that depends on the location of the buyer. (It does not specifically address the question of whether that tax should go to the buyer's tax jurisdiction of the seller's tax jurisdiction.)

14. IS THE PROPOSAL TECHNOLOGICALLY FEASIBLE UTILIZING WIDELY AVAILABLE SOFTWARE TO ENABLE TAX COLLECTION? IF SO, WHAT ARE THE INITIAL COSTS AND THE COSTS FOR REQUIRED UPDATES, AND WHO IS TO BEAR THOSE COSTS?

The proposal is technologically feasible. A few essential features are not currently available in today's software Costs would be relatively small, and would be borne by vendors.

15. DOES THE PROPOSAL PROTECT THE PRIVACY OF PURCHASERS?

Yes, the proposal is designed to protect the privacy of purchasers, as well as vendors.

16. DOES THIS PROPOSAL RESPECT THE SOVEREIGNTY OF STATES AND NATIVE AMERICANS?

The policy could be implemented while respecting existing rights of states or Native Americans.

17. HOW DOES THIS PROPOSAL TREAT LOCAL GOVERNMENTS' AUTONOMY AND THEIR ABILITY TO RAISE A GREATER OR LESSER AMOUNT OF REVENUES DEPENDING ON THE NEEDS AND DESIRES OF THEIR CITIZENS?

Local governments could be free to increase or decrease sales tax revenues as they see fit.

18. IS THE PROPOSAL CONSTITUTIONAL?

Yes. The proposal is constitutional.