Carnegie Mellon University
Research Showcase @ CMU

Department of Engineering and Public Policy | Carnegie Institute of Technology

Winter 1999

Making the Internet Fit for Commerce

Jon M. Peha
Carnegie Mellon University, peha@andrew.cmu.edu

Follow this and additional works at: http://repository.cmu.edu/epp

Part of the Engineering Commons

Published In
Issues in Science and Technology.

This Article is brought to you for free and open access by the Carnegie Institute of Technology at Research Showcase @ CMU. It has been accepted for inclusion in Department of Engineering and Public Policy by an authorized administrator of Research Showcase @ CMU. For more information, please contact research-showcase@andrew.cmu.edu.

Issues in Science and Technology, National Academy Press, Winter 1999.

Making the Internet Fit for Commerce:

Electronic commerce needs new policies to enforce tax laws, protect privacy, deter fraud, and prevent illegal sales.

Jon M. Peha
Carnegie Mellon University
peha@ece.cmu.edu, http://www.ece.cmu.edu/~peha

The laws of commerce, which were established in a marketplace where sellers and buyers met face-to-face, cannot be expected to meet the needs of electronic commerce, the rapidly expanding use of computer and communications technology in the commercial exchange of products, services, and information. E-commerce sales, which exceeded $30 billion in 1998, are expected to double annually, reaching $250 billion in 2001 and $1.3 trillion in 2003. In addition, by 2003 the Internet will compete with radio to be the third largest medium for advertising, surpassing magazines and cable television. On-line banking and brokerage is becoming the norm. In early 1998, 22 percent of securities trades were made online, and this figure is rising rapidly. Now is the time to review and update the laws of commerce for the digital marketplace.

In any commercial transaction, there are multiple interests to protect. Buyers and sellers desire protection from transactions that go wrong due to fraud, defective products, buyers that refuse to pay, or other reasons. Buyers and sellers may also want privacy, limiting how others obtain or use information about them or the transaction. Governments need effective and efficient tax collection. This includes sales or value-added taxes imposed on a transaction as well as profit or income taxes imposed on a vendor. Finally, society as a whole has an interest in restricting sales that are considered harmful such as the sale of guns to criminals.

The legal, financial, and regulatory environment that has developed to protect buyers, sellers, and society as a whole is inconsistent with emerging technology. When purchases are made over a telecommunications network rather than in person, there is inherent uncertainty about the identity of each party to the transaction and about the purchased item. Furthermore, it is difficult for either party to demonstrate that transaction records are accurate and complete. This results in uncertainty and potential conflict in four critical areas: taxation, privacy protection, restricted sales such as weapons to criminals and pornography to minors, and fraud protection.

Telephone and mail order businesses face similar problems, but e-commerce is different. With mail order, buyer and seller know each other's address, so tax jurisdictions are clear, and perpetrators of fraud and sellers of illegal goods can be traced. This is not true with e-commerce. Mail order revenues are a negligible fraction of the economy, so the fact that sales taxes are rarely collected for mail order is tolerable. E-commerce revenues will be significant. Current law is particularly inapplicable to e-commerce of information products such as videos, software, music, and text, which can be delivered directly over

the Internet. These sales produce no physical evidence such as shipping receipts or inventory records. Auditors cannot enforce tax law. Postal workers cannot check identification when making a delivery. And if either party claims fraud, it may be impossible to retrieve the transmitted item, prove that the item was ever transmitted, or locate the other party.

Two schools of thought have emerged about how to deal with e-commerce conflicts. One is that the infant industry needs protection from regulation. Lack of government interference has helped e-commerce grow, and heavy-handed regulation could cripple its burgeoning infrastructure and deny citizens its benefits. This philosophy underlies the position that all e-commerce should be tax-exempt, that all Internet content should be unregulated, and that consumers are sufficiently served by whatever privacy and fraud protections develop naturally from technological innovation and market forces. Proponents call this industry self-regulation.

Others argue that policies governing traditional commerce evolved for good reasons and that those reasons apply to e-commerce. They warn of the dangers in having different rules for different forms of commerce. If digitized music purchased online is tax-free and compact disks purchased in stores are taxed, then e-commerce is favored, and consumers who cannot afford Internet access from home suffer. Moreover, if a particular sale is illegal in stores but is legal on-line, then e-commerce undermines society's ability to restrict some purchases.

The problem is that rules developed for traditional commerce may not be applicable or enforceable with e-commerce. To meet old objectives, proponents push additional laws, sometimes with significant side effects. For example, the state of Washington considered legislation to impose criminal penalties on adults who make it possible for minors to access pornography on the Internet. Because there is no perfect pornography filter, this could effectively ban Internet use in schools and prohibit a mother from giving her seventeen-year-old son unsupervised Internet access from home. Australia prohibited Australian web sites from displaying material inappropriate for minors, thereby denying material to adults as well. Similarly, laws have been proposed to insure that sales taxes are always collected except when transactions are provably tax-exempt. Some proposals include unachievable standards of proof, forcing vendors to tax all sales. Worse, laws could make tax collection so expensive that e-commerce could not survive.

Policymakers are often forced to choose between conflicting societal goals--for example, between collecting taxes and promoting valuable new services--because policies and institutions are not equipped to meet both objectives. This need not be the case. The United States can devise a system that protects against misuse of e-commerce without stifling its growth.

Pornography, cryptography, and other restrictions.

The most prominent e-commerce controversy is the easy availability of pornography on the Internet. The draconian solutions are to censor material intended for adults or deny minors Internet access. In the 1996 Communications Decency Act, Congress penalized those who provide indecent material to minors. The US Supreme Court found the law unconstitutional because it would interfere with communications permitted between adults. The fundamental problem is the inability of vendors to ascertain a customer’s age.

Congress passed a less restrictive version in 1998 that affects only commercial web sites. It allows pornography vendors to assume that customers are adults if they have credit cards. This protects the financial interests of pornographers, but it allows minors with access to credit or debit cards to obtain pornography without impediment and prevents adults with poor credit from doing so. This also undermines the privacy of adults who do not want pornography purchases in their credit-card records.

Other restrictions have been proposed in Congress to protect children, including bans on Internet gambling and liquor sales. Such restrictions might protect children, but they would deprive adults of these services and reduce revenues for the respective industries. If these services do remain legal, some customers may insist on anonymity to participate, further complicating the need to check customers' ages. In addition, sales may be restricted in some jurisdictions and not others, which is problematic on the global Internet. For example, a New York court found that an online casino in the Caribbean violated New York laws, because New Yorkers can lie about their location and gamble. This court would shut down online casinos worldwide if they cannot determine whether customers are in New York.

Another reason to restrict sales is national security, as demonstrated in the debate over encryption. Law-abiding individuals use encryption to promote security, but criminals can use it to evade law enforcement. The United States does not regulate domestic sale of encryption software but tightly restricts its export. This is difficult to enforce. Encryption and products such as web browsers that include encryption are distributed over the Internet. Vendors must determine a buyer's nationality from an Internet address, which is an unreliable indicator. As a result, legal sales are hampered, while savvy foreign consumers can circumvent the rules.

National security issues also arise in other contexts. For example, legislation has been proposed to ban gun sales via the Internet because online gun vendors cannot check customer identification to prevent sales to criminals. This blanket prohibition would deny law-abiding citizens this convenience.

The alternative to broad restrictions is a system in which vendors can access and reasonably believe customer credentials, which might indicate whether a customer has a criminal record or is a minor or a U.S. citizen. Policymakers should penalize those who ignore credentials in cases where they could be available, and only those cases. A final point about sales restrictions: U.S. laws affect only U.S. vendors. If other nations do not impose and enforce similar laws, U.S. restrictions may achieve little or nothing.

Fraud and other failed transactions

Two problems must be addressed in order to provide protection against fraud. First, a transaction must create an incorruptible record. In traditional commerce, this can be accomplished with a paper receipt that is hard to forge. In e-commerce, one might reveal all information about the transaction to a third party. This is not always effective because the resulting record may not be trustworthy or available when needed. Moreover, this reduces the privacy of buyers and sellers.

Second, it must be possible to check credentials of other parties. Credentials could include a buyer's identity or just a credit rating. The chief technical officer of Internet software vendor CyberSource Corporation told Congress that in its early years, 30 percent of the company's sales were fraudulent; many buyers used other people’s credit-card

numbers, and assumed the identity of the rightful card-holder. CyberSource could not collect because the buyer could not be identified or located, and the item could not be retrieved. Buyers also need to check sellers' credentials for protection. For example, does that online pharmacy really have licensed pharmacists on staff?

Fraud would be more difficult if a unique identifier were embedded in each computer. Intel provided this feature in its latest processor, and Microsoft did the same in software. But the public immediately and loudly expressed opposition, because such identifiers could undermine privacy: Websites could use identifiers to track viewing habits of individuals in tremendous detail; an identifier could reveal authorship of documents created or distributed anonymously.

Another way to identity parties is through electronic signatures. Some commercial “certificate authorities” already provide such services. When a customer establishes an account, the certificate authority validates the customer's identity. The company then assigns the customer an electronic "secret key." Encryption techniques allow a customer to demonstrate that he knows this secret key by applying an electronic signature.

Unfortunately, there is no guarantee that certificate authorities operate honestly. Anyone can offer this service, and there is no government oversight. Consequently, it is not clear that their assurances should be legally credible. Moreover, today's commercial services often undermine privacy by presenting all information about a given customer, rather than just the minimal credentials needed for a particular transaction. They may do it because providing all the information makes it harder for a dishonest certificate authority to remain undetected, which is important given the lack of oversight.

Tax collection

A total of 46 states tax e-commerce, but taxes are collected on only 1 percent of e-commerce sales. This tax is simply unenforceable. As a result, e-commerce vendors have an unfair advantage, consumers without computers suffer, and state revenues are decreased. Many states depend heavily on sales tax revenues, so they want enforcement even if it damages e-commerce.Taxation of e-commerce has all the practical difficulties posed by restricted sales and fraud protection, and more. Sometimes, vendors must know about their customers to determine whether a given tax applies. For example, taxes may not be collected from customers in some locations or from licensed wholesalers. Such customers must supply trustworthy credentials, but this raises corresponding privacy concerns.

Neither sales tax on a transaction nor revenue tax on a vendor can be enforced without auditable records that are trustworthy. Traditional commerce generates paper trails of cash register logs, signed bills of sale, and shipping records that are difficult to alter or forge. E-commerce often produces only electronic records that are easily changed, especially when the transaction takes place entirely over a network. Without exchanging physical currency or touching pen to paper, people can buy stocks and airline tickets, transfer funds to creditors, "sign" contracts, and download magazines, music, videos, and software. The enormous increase in speed and decrease in costs in these transactions will make commerce without exchange of physical objectives 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.

Many policies neither support taxation nor protect privacy. Vendors in the state of Washington, for example, are expected to ask customers for their names and addresses, and collect taxes when customers give a Washington address or no address. Thus, anonymous out-of-state sales are taxed when they should not be. More important, name and address need not be verified or even verifiable, so customers within the state can establish false out-of-state accounts and easily evade taxes.

The 1998 Internet Tax Freedom Act prohibited new taxes on e-commerce for three years, although it does not affect existing taxes applicable to e-commerce, many of which predate computers. The Act established a commission to advise Congress by April 2000 on policies to enact before this three-year moratorium ends. The first year was spent arguing about who should be on the commission, and the commission never met. It is unclear whether this group will develop any policies, or if it does, whether its recommendations will be followed.

Privacy

There are already calls for legislation to further regulate the way today's credit-card companies, banks, stores, and others use and share personal information. Online vendors can capture even more information about their customers; for example, they know what products customers look at, not just what they buy. Privacy protection creates a particularly thorny dilemma because it could work against fraud protection, restricted sales, or taxation. These other objectives could be easier to achieve if transaction details were public.

On the other hand, some capabilities required for these other objectives, such as the ability to retrieve trustworthy credentials, are also essential when applying traditional privacy policies to e-commerce. For example, people are legally entitled to view their personal credit records and correct any errors. Applying this policy to e-commerce would fail unless a vendor can verify the identity of the person requesting access to this information.

Similar problems arise when different privacy policies apply to different users. For example, the 1998 Children's Online Privacy Protection Act prohibited vendors from collecting personal information from children without parental permission. Consequently, vendors must be able to distinguish minors from adults and to identify a minor's parent, which should require trustworthy credentials. (Today, a minor can lie about age without detection.)

Missing links

The most controversial issues of e-commerce have common underlying causes. Because buyers and sellers lack trustworthy information about each other during the transaction and auditors lack trustworthy records after the transaction, it has been necessary to compromise important policy objectives such as privacy and fair taxation. Rather than fight over which sacrifice to make, we should create an environment in which these objectives are compatible. We must supply the missing elements.

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, 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 do you know the third party's records will be correct, complete, and available when needed? Today, it is impossible, making problems inevitable.

Moreover, transaction records must go to third parties without undermining privacy. Today, many e-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 e-commerce. Parties to a transaction 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.

I propose a system that solves many of these problems. 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. To enable a true audit, outside entities must be involved in recording the transaction. This system therefore 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.

Technically, the system is based on public-key encryption. Each entity E gets a public key, which is available to everyone, plus a secret key, which only E knows. A message encoded using E's public key can only be decoded with E's secret key, so only E can decode it. E can "sign" a record by encoding it with E's secret key. If a signed record can be decoded with E's public key, then E must have signed the record. Public-key encryption operations are executed transparently by software.

Any person (or company) who 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 as either public or private. Public information can be used as credentials during transactions. Private information may be accessed later 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 U.S. citizenship as public information. Her nationality, public key, and account number are publicly displayed on the verifier's website. Auditors can check her identity if necessary. Vendors know only her verifier account number and citizenship, allowing her to purchase anonymously U.S. encryption software that is subject to 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 U.S. citizen. This would also enable her, for example, to purchase stock with both accounts without revealing that there is only one buyer.

For each verifier account, a relationship is established with one or more notaries. Some government agency must be informed of all verifier accounts and relationships with notaries. This prevents vendors from keeping multiple sets of records, and deciding later which to reveal. Then, e-commerce transactions can begin. In a transaction, all parties create a description of the relevant details using a standardized format. For a software purchase, the description might include the software title, warranty, price, date, time, and the 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.

Each party in a transaction 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 the record, 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. 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.

Entities that are not subject to audits, including most consumers, would be largely unaffected by this system. A customer who makes restricted purchases such as guns might be required to register once in person. Software executes other functions transparently.

Several companies 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, e-commerce 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? When a company is ensuring that tax laws are enforceable and keeping weapons from criminals, government must make certain. The federal government should support voluntary accreditation of verifiers and notaries. Only accredited firms should be used when generating records to comply with federal laws or to interact with federal agencies. Others are likely to have confidence in a firm accredited by the government, which could further bolster e-commerce, but private companies would be free to use unaccredited firms.

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.

Limited government oversight is needed to make this system work. Auditors must occasionally check randomly-selected records from notaries and verifiers to insure that nothing has been altered. Government also keeps track of the verifier and notary accounts held by each electronic vendor and any other parties subject to audit.

Many current laws and regulations require written records, written signatures, or written timestamps. Federal and state legislation should allow electronic versions to be accepted as equivalent when the technology is adequate. Contracts should not be unenforceable simply because they are entirely electronic. It should be possible to legally establish the date and time of a document with an electronic notary. A notice sent electronically should be legally equivalent to a notice sent in writing, when technology is adequate. For example, a bank could send a foreclosure notice electronically, provided that accredited verifiers and notaries produce credible evidence that the foreclosure was received in time. Similarly, electronic records of commercial transactions should carry legal weight when technology is adequate. For example, commercial vendors must show records to stockholders and tax auditors. The Securities and Exchange Commission, the Internal Revenue Service, and state tax authorities should establish standards for trustworthy electronic records using accredited verifiers and notaries.

Government could improve its own efficiency by using these systems. Congress took the first small step in 1998 by directing the federal government to develop a strategy for accepting electronic signatures. Government should use commercial services whenever practical, rather than developing its own.

The new approaches used to identify parties in e-commerce raise novel policy issues regarding identity. Who is responsible if a verifier incorrectly asserts that an online doctor is licensed? Certificate authorities already want to limit their liability, but such limits discourage use of appropriate technology and sound management. It should also be illegal for customers to provide inaccurate information to a verifier. If this inaccurate information is used to commit another crime such as obtaining a gun for a criminal, that is an additional offense. Other identity issues are related to electronic signatures. It should be illegal to steal someone's secret code, which would enable forgery of electronic signatures. It should even be illegal to deliberately reveal one's secret code to a friend. Forgery and fraud are illegal, but these acts that enable forgery and fraud in e-commerce may now be legal because they are new.

Accredited and unaccredited verifiers and notaries should be required to notify customers about privacy policies, so consumers can make informed decisions. Vendors could be allowed to sell restricted products such as pornography, encryption software, guns, and liquor if and only if they check credentials and keep verifiable records where appropriate. For dangerous physical goods such as guns, double checking is justified. Online credentials would include name, mailing address, and criminal status; the name would be verified again when the guns are delivered.

One of the most difficult outstanding issues is to determine when a vendor must collect sales tax and to which government entity it should be paid. At present, taxes are collected only when buyer and seller are in the same state. Policies should change so that collection does not depend on the location of the seller, because too many e-commerce businesses can easily be moved to avoid taxes. This forces vendors to collect taxes for customers in all jurisdictions. There are 30,000 tax authorities in the United States with potentially different policies; monitoring them all is a costly burden. State-wide or regional clearinghouses should accept taxes from vendors and distribute them to appropriate local authorities. Tax rates and policies could be harmonized throughout these regions (such as states), although there would be opposition, particularly from cities, as they often have higher sales tax. At minimum, it would help if product categories were standardized; if two jurisdictions may tax food at different rates, but their definitions of food would be identical.

A vendor still cannot tell a customer's location (and vise versa), especially with transactions that do not involve tangible products. A verifier could provide trustworthy static information, such as billing address or tax home, but not actual location at the time of purchase. Taxing based on static information is more practical, although a few people may manipulate this information to evade taxes. At minimum, each party should state its location in a notarized transaction record, so retroactive changes are detectable.

Now is the time to devise policies that are both technically and economically appropriate for e-commerce - before today's practices are completely entrenched. This can only be accomplished by addressing fundamental deficiencies in the e-commerce system rather than by debating individual controversies in isolation. This includes creation of commercial intermediaries. Verifiers can provide trustworthy credentials, and notaries can insure that transaction records are complete and unaltered. Dividing responsibilities for these functions among competing notaries and verifiers will capture enough information for tax auditors and law enforcement agents to pursue illegal activities without sacrificing the privacy of the law-abiding.

To make this happen, government should develop accreditation procedures for verifiers and notaries. It should update laws and regulations to allow electronic records to replace written records when and only when the technology is adequate. Government should also use these new services. It should develop new policies on taxation and restricted sales that are consistent with e-commerce. And for those who try to exploit the new technology illegally, criminal codes should provide appropriate punishments.

Recommended Reading

1. N. Asokan, P. A. Janson, M. Steiner, M. Waidner, "The State of the Art in Electronic Payment Systems," *IEEE Computer*, Vol. 30, No. 9, Sept. 1997, pp. 28-35.
2. D. Chaum, "Achieving Electronic Privacy," *Scientific American*, Aug. 1992, pp. 96-101.
3. W. J. Clinton, A. Gore, *A Framework for Global Electronic Commerce*, July 1, 1997, www.iitf.nist.gov/eleccomm/ecomm.htm
4. Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, www.ftc.gov/reports/privacy3/index.htm
5. M. Hellman, "The Mathematics of Public-Key Cryptography," *Scientific American*, Aug. 1979, pp. 146.
6. R. J. Hillman, "Securities Fraud: The Internet Poses Challenges to Regulators and Investors," US General Accounting Office Report GAO/T-GGD-99-34, March 22, 1999, www.gao.gov/AIndexFY99/abstracts/gg99034t.htm
7. J. P. Morgan, A. Gidari, *Survey of State Electronic and Digital Signature Legislative Initiatives*, www.ilpf.org/digsig/digrep.htm
8. National Tax Association, Communications and Electronic Tax Project, Final Report, www.ntanet.org/ecommerce/final.pdf
9. J. M.Peha, *Proposal on Taxation of Electronic Commerce*, US Advisory Commission on Electronic Commerce, Nov. 1999, www.ece.cmu.edu/~peha/ecommerce.html
10. J. M.Peha, "Making Electronic Transactions Auditable and Private," *Proceedings of the Internet Society's INET-99*, June 1999, www.ece.cmu.edu/~peha/ecommerce.html
11. J. M.Peha, *Encryption Policy Issues*, Oct. 1998, www.ece.cmu.edu/~peha/policy.html
12. J. M.Peha, R. P. Strauss, "Primer on Changing Information Technology and the Fisc," *National Tax Journal*, Vol. L, No. 3, Sept. 1997, pp. 608-21, www.ece.cmu.edu/~peha/ecommerce.html
13. J. M.Peha, *A Modest Proposal for the Immodest Internet*, editorial on the 1996 Communications Decency Act, www.ece.cmu.edu/~peha/policy.html
14. M. A. Sirbu, "Credits and Debits on the Internet," *IEEE Spectrum*, Vol. 34, No. 2, Feb. 1997, pp. 23-9.
15. R. P. Strauss, “Further Thoughts on State and Local Taxation of Telecommunications and Electronic Commerce,” *State Tax Notes*, Oct. 25, 1999, www.heinz.cmu.edu/~rs9f/speech.html