To appear in *Issues in Science and Technology,* National Academy Press, Fall 1999.

Addressing Policy Issues of Electronic Commerce:
Taxation, Privacy, Fraud Protection, And Restricted Sales

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

Abstract

The laws governing commerce were established when buyer and seller met face to face. In *Electronic commerce*, goods and services are exchanged across a communications network, raising difficult new problems with respect to *taxation, privacy, fraud protection*, and *restricted sales* (such as pornography to minors, or weapons to criminals). Limitations of today's electronic commerce infrastructure force policy-makers to balance competing objectives. For example, do we undermine an accepted policy objective, or hobble the growth of electronic commerce? The controversies in these four critical areas share a common origin. When other parties involved in a transaction are remote, it is difficult to obtain trustworthy information about the transaction, and to create a verifiable record. This paper discusses these controversies in detail. It then proposes steps that policy-makers and industry could take to address the underlying problems in our electronic commerce infrastructure, thereby reducing or eliminating many of these policy dilemmas.

Section 1: Introduction

Electronic commerce, which is the commercial exchange of products, services, and information over a telecommunications network, is becoming a viable alternative to traditional face-to-face transactions. Over 30 billion dollars of products were sold via electronic commerce in 1998. Forrester Research estimates that these sales will double every year, reaching roughly 250 billion dollars in 2001, which is comparable to the US auto and telecommunications industries. By 2003, annual electronic commerce sales are projected to reach 1.3 trillion dollars. Transactions without payments are also lucrative. Jupiter Communications estimates that by 2003, the Internet will by vying with radio for the third biggest medium for advertising behind newspapers and broadcast television; that means the Internet will soon surpass magazines and cable television. On-line banking and brokerage are becoming the norm. There were 4.3 billion dollars worth of on-line securities trades in 1998, and this figure is expected to reach 1.3 trillion dollars in 2003. Policies made today regarding such electronic commerce practices will probably remain in place as these practices become an increasingly important aspect of the world's economy and information infrastructure.

The legal, financial, and regulatory environment of traditional commerce has developed over time to protect buyers, sellers, and society as a whole. However, this environment is not yet consistent with the emerging technology. When one buys something over an electronic network rather than in person, there is inherent uncertainty about the identity of the other party in the transaction, and the purchased item. (Even where businesses derive revenues from advertisers rather than customers, we still consider these to be purchased items.) Furthermore, it is more difficult for either party to demonstrate that records of the sale are accurate and complete. This is the root of some of the most difficult and controversial issues of electronic commerce, such as

- appropriate and efficient collection of sales and income tax,
- protection of consumer and vendor privacy,
- prevention of restricted sales, e.g. weapons to criminals, or pornography to minors,
- fraud protection for both vendors and consumers.

In each of these four areas, two fundamental schools of thought have emerged. One position is that we should protect this infant industry and encourage innovation by refraining from any kind of regulation. Lack of government regulation so far has clearly helped the Internet, the WWW, and electronic commerce to grow. Heavy-handed regulation could cripple our growing infrastructure, and deny us the benefits it could provide. This philosophy underlies arguments that all electronic commerce transactions should be tax-exempt, that all WWW content should be unregulated, and that consumers will be sufficiently well served with whatever privacy and fraud protections develop naturally from technical innovation and market forces (i.e. from industry "self regulation"). On the other hand, others would argue that those policies and regulations for traditional commerce evolved for good reason, and those reasons are equally valid with electronic commerce. Moreover, there are dangers in having different rules for different forms of commerce. For example, if one can purchase digitized music over the Internet tax-free, but taxes are collected when music is sold in stores, then society is inappropriately favoring the electronic commerce purchase. Worse, if a sale would be illegal in a store, but the law does not apply over a network, then electronic commerce has undermined society's ability to restrict sales.

The problem is that rules and regulations developed for traditional commerce may not be applicable or enforceable in the context of electronic commerce. Consequently, proponents push for additional laws, some of which create unintended burdens. For example, some states like Washington have considered legislation that would impose criminal penalties on adults who make it *possible* for minors to gain access to pornography on the Internet. Because there is no perfect filter for pornography, this would effectively ban Internet use from schools, and would even make it illegal for a mother to give her seventeen-year-old son unsupervised access to the Internet from home. Australia is considering legislation to address the problem by prohibiting Australian-based web sites from publicly displaying material that is inappropriate for minors, thereby denying the material to adults as well. Similarly, some proposed laws are intended to make tax evasion difficult in electronic commerce by forcing a vendor to provide solid proof that a transaction is really tax-exempt. If such standards can never be met, vendors are forced to collect state sales taxes on all transactions, even those that are legitimately tax-exempt. Even stricter requirements could make electronic commerce so expensive that it could not survive.

This paper will argue that many of the controversies described above are not inherent in electronic commerce or the technology that enables it. Policy-makers are forced to choose between conflicting societal goals, like collecting taxes versus promoting valuable new services, because our current policies and institutions were not designed to meet both objectives. This need not be the case.

Section 2 will describe both sides of the controversies surrounding electronic commerce in greater detail. It will also show that they are all rooted in the same deficiencies of the existing infrastructure. Section 3 will show that there are ways to address these deficiencies that involve the establishment or expansion of new commercial sectors, which will play a vital role in our commercial infrastructure. Section 4 will describe how policy-makers can provide a catalyst for these new commercial services to emerge. The paper is concluded in Section 5.

Section 2: The Controversies

In any commercial transaction, there are multiple interests to protect. Buyers and sellers desire protection from a transaction that goes wrong. We refer to this as fraud protection, but it could include other cases where the transaction does not go as expected, such as when a product is defective, or when payment is never received. Buyers and sellers may also desire privacy protection, whereby they can limit how others obtain or use information about themselves or the transaction. Governments have an interest in effective and efficient tax collection. This includes sales or value-added taxes imposed on a transaction, and profit or income taxes imposed on a vendor. Finally, society as a whole may have an interest in restricting sales that are considered harmful, such as guns to criminals. There have been controversies in each of these four areas, as will be described in Sections 2.1 through 2.4.

Section 2.1: Restricted Sales

Some sales are restricted for their effects on the community at large. The most common justifications are that some sales might put dangerous tools in the hands of potential criminals, or might put inappropriate material in the hands of children.

One of the more celebrated controversies related to electronic commerce has concerned the availability of pornography on the Internet. As described in Section 1, the Draconian solutions are to censor material intended for adults, or to deny minors access to the Internet. The US Congress tried to keep pornography from minors through the 1996 Communications Decency Act, which imposed heavy penalties on those who provide indecent material to minors. The US Supreme Court determined that the law is unconstitutional because it would also interfere with legitimate communications between adults. Thus, the root of the problem is the inability of vendors to ascertain the age of their customers. Other proposed laws have held the Internet Service Providers (ISPs) accountable as well. This is even more problematic because ISPs cannot always determine what information they are carrying, any more than the Postal Service can know what is contained in undeveloped film that is mailed. Holding vendors or ISPs accountable for information that they cannot verify would have broad unintended consequences. Allowing them to accept the word of their customers that a transaction would not transfer pornography to minors would be completely ineffectual. This gives policy-makers a serious dilemma. Some place their hopes in filtering software, which is inherently imperfect; such software will allow some pornography through, block some useful information (such as educational material on AIDS), or typically, both.

The same dilemma resurfaced in 1998, when Congress passed a more restricted version of the Communications Decency Act that would only affect commercial WWW sites. (The Supreme Court has not yet ruled on this version.) This legislation allows the Internet pornography industry to assume that customers are adults if and only if they have a credit card. Unfortunately, credit ratings are only loosely correlated with age. This practice

would probably protect the financial interests of pornographers, but it would still allow minors with access to credit cards to obtain pornography without impediments, while limiting information available to adults with poor credit ratings, and adults who do not want credit card companies to chronicle their interest in pornography. Thus, there is also a privacy concern.

There are other restrictions intended to protect children. For example, minors are prohibited from gambling or buying alcohol, but on-line casinos and liquor vendors may be unable or unwilling to apply those laws. Moreover, customers may be unwilling to sacrifice anonymity. One bill before congress would ban on-line gambling entirely, thereby protecting children, but depriving adults of this form of entertainment, and reducing revenues for the industry. Another bill, entitled the Juvenile Justice Act, would ban electronic commerce in alcohol to protect children. (For sale of physical objects such as bottles of liquor, on-line vendors could ship products to a trusted third party who would check identification cards in person before handing over products, although this would significantly increase transactions costs and reduce convenience. For sale of information products like pornographic images, this is not practical.)

Sales may be restricted in some jurisdictions and not others, which is problematic in the inherently global Internet. A New York court found that an on-line casino based in the Caribbean had broken New York laws because it is *possible* for New Yorkers to lie about their location and gamble. As the casino's lawyer said, his client "used the best technology we have ... but it didn't matter to the judge." This court would shut down on-line casinos around the world if they cannot determine whether customers are in New York.

Another reason to restrict sales is security. For example, a debate has raged over the distribution of strong encryption. Legitimate businesses and law-abiding individuals can use such encryption to promote security, but criminals and terrorists can use it to evade law enforcement. The US currently does not regulate domestic sale of encryption, but places tight restrictions on exports. Since products with encryption such as WWW browsers are often distributed over the Internet, vendors are forced to apply restrictions that depend on the citizenship or location of the recipient. Such vendors typically look at the IP (Internet Protocol) address of the recipient, which is a poor substitute for citizenship credentials. This puts impediments before valid sales. Moreover, these impediments can be overcome by a knowledgeable user, even if that user is a criminal or terrorist. This is one reason (albeit not the only reason) that the Federal Bureau of Investigations (FBI) Director Louis Freeh and many members of congress are seeking to impose tight restrictions on domestic sales as well as exports.

The same security issues arise in other contexts. For example, Senator Diane Feinstein has advocated legislation restricting on-line information on bomb-making, and Senator Charles Schumer has proposed a ban on gun sales using the Internet. Thus, because gun vendors using the Internet cannot check customer identification cards to prevent sales to criminals, law-abiding citizens could lose this convenience.

A meaningful restriction on sales requires creation of a system whereby vendors can access and reasonably believe customer credentials, which might indicate whether a customer has a criminal record, or is a minor, or a US citizen. Policy-makers should impose penalties on those who ignore credentials in cases where reliable credentials are or could be available. In other cases, such penalties may be ineffectual, or worse.

For all of these restrictions, it should be noted that US laws only affect US vendors. If other nations do not impose and enforce similar laws, then US restrictions may achieve

little or nothing. This must also be considered when deciding whether to impose these restrictions.

Section 2.2: Fraud and Other Failed Transactions

An effective system of commerce must protect both parties from fraud, and other cases where one party does not receive what he or she expects. In electronic commerce, this is problematic because neither party can see what they will receive. Two problems must be addressed. First, each party needs the ability to determine if the distant party is who or what they claim to be. The needed credentials could include the other party's identity, or just a credit rating, or whether the other party has a credible seal of approval. Second, a transaction must create some kind of proof-of-purchase receipt or record.

We begin with the former problem of establishing another party's identity or credentials. For example, CyberSource Corporation sells software over the Internet. Its Chief Technical Officer testified before Congress that in its early years, 30% of its "sales" were fraudulent; thieves were finding valid credit card numbers, and assuming the identity of the card-owners. These thieves would download software, and the company could never collect. Credentials are also needed for quality control. For example, there are vendors that prescribe and sell drugs over the Internet who have no licensed doctors or pharmacists on staff, and who do not follow established safety procedures.

Fraud would be considerably more difficult if there were a unique identifier embedded in every one's computer system. Intel provided this feature in their latest processor, and Microsoft did the same in their software. The public outcry over these identifiers was strong and immediate. Despite the value of such an identifier, consumers demanded the ability to disable these features, because they can also be used to undermine privacy. Microsoft could use them to help determine what software every computer system is using, and whether that software was purchased from Microsoft. Web sites could use these identifiers to track the viewing habits of individuals in tremendous detail. An identifier could even make it possible to determine authorship of documents that were supposedly created or distributed anonymously. Both the benefits and dangers of this approach became apparent when law enforcement used this feature to track down the creator of the Melissa virus, which interfered with Internet users around the world in early 1999. Intel and Microsoft were both nominated for the infamous 1999 Orwell Awards for threatening the privacy of individuals, and Microsoft "won." Whether the bad press will have any impact on sales remains to be seen.

Another way to identity parties is to use *electronic signatures*. Some commercial *certificate authorities* already provide credential services. When a customer establishes an account, the certificate authority investigates the customer's identity. The company then assigns the customer a "secret key." Encryption techniques allow a customer to demonstrate that it knows the secret key by applying an electronic signature without actually revealing they key. Assuming that the key has not been accidentally or deliberately revealed to an outsider, these firms can thereby verify a customer's identity. Unfortunately, there is little guarantee that these certificate authorities operate honestly. Any one can offer this service, and there is no government oversight. Consequently, it is not clear that their assurances will carry the credibility in legal proceedings that the technology might reasonably allow. Moreover, today's commercial services typically undermine privacy by presenting all of the information about a given customer, rather than just the minimal set of needed credentials. Providing all of the information makes it more difficult for a dishonest certificate authority to present fraudulent information without detection, which is important given the lack of oversight on certificate authorities.

The other problem to be addressed is creating an uncorrupted record of the transaction. For example, such a record would allow a customer to show that she had purchased a particular software package from a given vendor at a given price within the last seven days, thereby allowing her to demand compensation if the software is defective. In traditional commerce, this can be accomplished by creating a paper receipt that is hard to forge. In today's electronic commerce, this often involves revealing all of the transaction information to a "trusted" third party, such as a credit card company. This inherently reduces the privacy of buyers and sellers, and the impact is magnified if these third parties can use this information to advantage. Congress is currently considering legislation that would restrict use of this personal information, particularly in cases where one company has multiple business interests (credit card operations, department stores, insurance, banks, etc.), and can use information collected in one subsidiary to market products and services in another.

Section 2.3: Taxation

In 45 out of 50 US states, when some one residing in the state makes purchase, whether it is in a store or over the Internet, sales tax must be paid to the state. However, only 1% of Americans who make purchases on the Internet pay any sales tax, because current laws are not enforceable. Thus, electronic commerce vendors gain an unfair advantage, and State revenues are diminished.

Taxation of electronic commerce raises all of the difficult issues underlying restricted sales and fraud protection, and the difficulties are amplified. Dependable transaction records are again required. Whether one is applying a sales or value-added tax to each transaction, or applying a revenue or profit tax to a vendor, enforcement is only possible when a reliable audit trail is generated. This time, the records must be reliable even if both buyer and seller wish to alter or erase them. Moreover, vendors must typically know something about their customers to determine whether to apply a given tax, raising all of the same needs for reliable credentials, and corresponding privacy concerns. For example, a vendor is not expected to collect taxes when it sells to a customer residing in a state where the vendor has no operations. Similarly, a wholesaler should not collect taxes when selling to a retailer.

Traditional commerce achieves auditability by generating papers that are difficult to alter or forge, such as cash register logs, signed bills of sale, and shipping records. This is difficult for electronic commerce, and it is presently impossible in cases where the transaction takes place entirely over a network, with no exchange of physical objects. For example, without sending physical currency or touching pen to paper, consumers may purchase stocks and airline tickets. They may transfer funds to creditors, and "sign" contracts. They may download news articles, music, videos, and software. (Why pick up a videocassette or compact disk at a store when you can download the information from the Internet?) The enormous potential to increase speed and decrease transaction costs in these cases will make this a common practice.

Such transactions create two problems for tax auditors. First, the transactions leave no physical evidence such as shipping records behind for law enforcement investigators. Second, unlike a physical product, information can be sold multiple times. Thus, one cannot corroborate revenue figures by looking at inventory. Auditors must depend entirely on transaction records. If transaction records exist only in computer memories that can be changed without risk of detection, any policy that requires such records for enforcement is doomed. Consequently, some have argued that we should not try to tax electronic commerce.

State and local governments are affected most, creating a natural tension between state and federal policy. For many states, sales tax is a critical source of revenues. As electronic commerce becomes more common, failure to collect these taxes will have a significant impact. Most states attempt to craft compromise policies that allow them to collect taxes as they would for mail order sales. Consider Washington State's approach. Mail-order vendors are required to collect taxes only for in-state customers. Electronic commerce vendors in Washington are expected to ask customers for their name and address, and taxes are collected if and only if the address given is within Washington, or if customers do not provide this information. Thus, anonymous sales outside the state are taxed when they should not be. More importantly, the name and address information need not be verified or verifiable, allowing customers within the state to establish an account with false information and easily evade sales taxes.

In 1998, the US Congress passed the 1998 Internet Tax Freedom Act, which prohibited the imposition of *new* sales taxes on electronic commerce for three years. From the press releases of the time, one might believe that the problem is solved. In fact, not only is this a temporary respite from the issue, but it does not affect the many existing tax laws that already apply to electronic commerce, many of which were in place long before computers existed. The Act established a new Advisory Commission on Electronic Commerce, which was tasked with crafting a new policy to be enacted before this three-year moratorium ends. The first year was spent arguing in and out of court about who should be on the commission, as the results will strongly depend on the number of members sympathetic to the electronic commerce industry and the number sympathetic to state governments. It is unclear whether this group will ever actually attempt to develop policies, whether it will reach consensus, or whether any resulting recommendations will be enacted.

Section 2.4: Privacy

Modern information technology makes it much easier to assemble and exploit personal information on a targeted individual or collection of individuals. Not surprisingly, legislators are considering these privacy issues anew in many contexts. For example, Congressman Ed Markey is pushing for more privacy protection of medical records and financial records. Congress is also currently considering legislation regulating how on-line vendors can collect and use personal information. In each context, the basic issue is whether these firms will inform customers about the personal information that is collected and how it is used, and whether they will give customers a choice of whether or not to permit these activities.

As the previous sections demonstrate, in some ways, the privacy objective sits in opposition to fraud protection, restricted sales, and taxation. These other objectives are often easier to achieve if the details of electronic commerce transactions are public.

However, some of the capabilities needed to achieve these other objectives, like the ability to retrieve reliable credentials, are also essential if some traditional privacy policies are to apply with electronic commerce. For example, in the context of personal credit records, a customer must be able to view all personal information that has been collected about her, and to correct any errors. Otherwise, the errors can grow and propagate. Applying a similar policy to electronic commerce would succeed only if a vendor can verify the identity of the person requesting access to this personal information. Without this capability, mandating such a policy might be equivalent to prohibiting the collection of personal information, even with consent, because the requirement could never be met.

Similar problems arise when different privacy policies are established for different users. For example, when Congress passed the 1998 Children's Online Privacy Protection Act, it established protections for minors and only for minors. As with restricted sales, vendors must be able to differentiate minors from older customers. The vendor is allowed to collect personal information on children with parental permission, which means the vendor must also be able to identify the parent. Following this law will be problematic.

Section 3: A New Approach

Section 2 described numerous controversial issues of electronic commerce, with common underlying causes. Because parties do not have access to reliable information about each other during the transaction, and auditors do not have access to reliable records after the transaction, it is often necessary to compromise one or more important policy objectives. Rather than fight over which sacrifice to make, we should be creating an environment in which these objectives are compatible. This requires the creation of new entities, which are described below.

Section 3.1 described the system's requirements. Section 3.2 provides an overview of the proposed system, while Sections 3.3 to 3.5 describe key aspects in greater detail. The limitations of this system are presented in Section 3.6.

Section 3.1: Today's Missing Elements

There must be a method of retrieving reliable credentials during the transaction. Records must be generated for each transaction, some of which may be randomly selected for audit. From these records, it must be possible for an auditor to later determine whether relevant laws were followed. For example, for sales tax purposes, records must include sufficient information to determine whether a transaction is subject to sales tax, the amount of the tax, the tax year or period, and the local, state, or federal entities to which taxes are due. Any attempt to forge, destroy, or retroactively alter transaction records must face a significant risk of detection.

When records can be changed at will, as is often the case with electronic commerce, it is not sufficient for the parties to a transaction to keep transaction records. An auditor does not always have the ability to review all copies, and even if the auditor can, the parties could still change records retroactively if they cooperate. This could allow them to cover up restricted sales, reduce their tax debts, or move a transaction to a different tax period. Clearly, there must be some kind of trusted third party to make transaction records reliable.

This must be achieved without undermining privacy. In the current system in which credit card companies are usually the trusted third parties, customers and merchants entirely surrender their privacy to the credit card company, and often to each other. To meet standard privacy objectives, parties in a transaction should have to reveal nothing beyond the credentials necessary for that particular transaction. Other than authorized auditors, no one should have access to any information on others except those credentials deliberately declared for a given transaction. It should even be impossible to determine whether some one else has engaged in transactions, or with whom they have engaged in transactions.

Given that current systems offer so little protection, the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants have taken a different approach. A designated entity will certify that companies are trustworthy based on their stated operational policies regarding business practices, transaction integrity, and

information protection. Firms wishing to display the "Webtrust" seal must approach this entity with some kind of corroborative evidence that the firm's policies are satisfactory. It is assumed that the firm will continue to meet criteria thereafter, which may or may not be the case. While there may be some advantages to a certification procedure, relying too heavily on such an approach can give customers, vendors, and tax auditors a false sense of security.

Section 3.2: Overview of Proposed System

We now present one possible system that solves many of the above problems. Conceptually, the system works as follows. All parties agree on the specifics of a transaction, and create a record of it. Each party receives a copy of the record signed by all parties. A party that is subject to audits then *notarizes* its copy in a manner that allows subsequent audits. (See Peha 1999 for a more detailed technical description.)

To provide true auditability, a number of outside entities must be involved in recording transaction records. In addition to buyers and sellers, the system consists of *verifiers*, *notaries*, and *auditors*. Verifiers are responsible for checking the identity of all parties, and verifying their credentials. Every transaction record passes through a notary, who establishes a time and date, and must insure that any alterations after the transaction record is notarized will be detectable. This is analogous to a notary public's function for paper documents. Auditors oversee customers, as well as verifiers and notaries.

Separating verifier and notary functions is crucial. Verifiers typically know the true identity of a customer. Notaries know whether an entity is notarizing transactions, and perhaps some information about those transactions. An entity that served as both a verifier and a notary (like a typical credit card company) would therefore know that a given customer is processing transactions, undermining the customer's privacy.

Entities that are not subject to audits, i.e. most customers, would be largely unaffected by the proposed system. Most would register with verifiers. A customer that wants the ability to make purchases that are restricted such as alcohol or strong encryption may have to register in person. Others could register over the Internet with the click of a mouse button. Standard software packages, perhaps embedded in WWW browsers, should handle the rest transparently.

Technically, the system is based on *public key encryption*. Each entity E gets a public key, which is publicly available to every one, and a secret key, which only E knows. If a message is encoded using E's public key, then it can only be decoded with E's secret key, which means only E can decode it. This protects communications to E from eavesdropping. Conversely, E is the only one who can encode a message with E's secret key; anyone can verify the result by encoding it with E's public key and producing the original message again. This is the basis of E's *digital signature*.

Section 3.3: The Verifier

Each customer must *register* with one or more verifiers before using the system. To register, a customer informs the verifier of its public key. (The verifier need not know its secret key.) The customer has the option of providing additional information, which it may designate as 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 information.

For example, a registering customer provides his name and social security number as private information, and his US citizenship as public information. This is done by presenting official identification documents in person. His nationality, public key, and account number are placed in public view on the verifier's web site. He can now purchase software without showing identification, including American software with export control restrictions. Auditors can determine his identity if necessary, but software vendors know only his verifier account number. No one else knows his secret key. The customer also registers with a second verifier. This time, he declares as public information that he is a software retailer, which allows him to avoid certain sales taxes, but excludes his nationality.

By creating two distinct verifier accounts, no one can determine that there is a buyer that is both a software retailer and has US citizenship. He can also buy stock in a given company from multiple accounts without the seller realizing that there is only one buyer. Finally, if one verifier is down, he can use the other. So transactions are still traceable, the customer must inform the auditor of both of his verifier accounts.

Today's commercial certificate authorities could expand their service offerings to serve this verifier function. By doing so, they would grow from an obscure niche market to a crucial service in the financial infrastructure of electronic commerce, just as banks and credit card companies are critical to traditional commerce.

Section 3.4: The Notary

For each verifier account, a customer also establishes a relationship with one or more notaries. The customer informs the auditor of all of its verifier accounts, and respective relationships with notaries. Each transaction from a given verifier account must be processed by one (and only one) of these notaries.

All parties in a transaction create a Description containing all relevant details of the transaction using a standardized format. For example, if this transaction is a software purchase, a Description might include a description of the software, the price, the date, the time, and the current (self-stated) location of buyer and seller. A Transaction Record consists of the Description with the digital signatures of all parties, and the verifier account of each party. This is equivalent to a signed bill of sale. Any one examining the Transaction Record can prove that all parties agreed to it.

Each party in a transaction notarizes its version of the Transaction Record. This makes it possible to audit one customer without viewing the records of other customers. The notary adds a timestamp, and processes the record. It is possible to establish a process whereby the notary cannot decode any portion of the record, so privacy is protected. Moreover, once a record is processed, any subsequent change would be detectable to an auditor, even if all parties to the transaction and the auditor cooperate in the attempted falsification. The party notarizing a record must also provide proof of its identity. This allows the notary (and an auditor) to assemble all records notarized by a given vendor, so no records can be deliberately "forgotten."

The notary also sends a receipt back. Anyone with a copy of both a notarized record and the associated receipt can verify the identity of the party who notarized the record, the time at which it was notarized, and that the information in the record has not been altered.

Notaries would also be an important new commercial sector. Several notaries already operate on the Internet, offering *some* of the necessary functions described above. In particular, *current notaries cannot produce a list of all notarized transactions for a given vendor*, and thereby prove that no transactions were "forgotten." 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 and regulations.

Section 3.5: The Auditor

A new corps of government auditors is needed to make this system work. Auditors must randomly check records from notaries and verifiers to insure that nothing has been altered. (With appropriate technology, alterations are detectable.) Auditors also keep track of the verifiers and notary accounts held by each electronic commerce vendor, and any other parties subject to audit. Thus, when it is time to audit a specific vendor, the auditor knows whom to contact.

Once a transaction has been notarized, it is not possible to alter or delete records of that transaction without risking detection from the auditor, even if buyer, seller, verifier, and notary conspire to do so. To prevent an auditor from safely joining a conspiracy, there could be multiple auditors. Generally, one auditor will not know about the actions of other auditors, so it is possible that the same customer will be audited twice. At this point, if one finds fraud and the other did not, the matter would be investigated further, possibly revealing any auditor malfeasance. Thus, the only way to falsify records safely is to involve all of the auditors in the conspiracy.

Section 3.6: Limitations of the Proposed System

The system above has three noteworthy limitations, which can influence policy. Indeed, these limitations are currently shared by all practical electronic commerce systems.

With this system, an attempt to falsify records is detectable if at least one party to each transaction initially records it honestly, even if all parties would later conspire to alter the records. However, it is impossible to detect the case where all parties agree to falsify records at the time of a transaction. This limitation is not specific to electronic commerce; it applies to commerce in the physical world as well. For example, if an item is purchased in a store, and the customer and store-owner agree to ring up the sale at a lower price, the cash register receipts will not reveal any anomaly to an auditor. Given that the problem is not unique to electronic commerce, it has no new policy implications.

A difficult problem for any electronic commerce system is determining the exact location of buyers and sellers. Under current laws, a vendor is typically obligated to pay state sales tax if and only if both buyer and seller are active in the state at the time of the sale. The verifier described in Section 3.3 can provide reliable static information, like where a customer's billing address is, but not instantaneous location. Communications networks are often deliberately designed to obscure this information. Knowing an Internet email address does not imply that one knows the owner's physical location. Location is not known in a telephone network when 800 numbers or call forwarding are used. New "personal communications" wireless systems are emerging in which the fact that the caller need not know the location of the called party is considered an important selling point. Policies must be designed around these limitations.

Finally, any system that uses cryptographic techniques like digital signatures has an inherent vulnerability. Good cryptographic codes are difficult to break, but individuals can always deliberately or accidentally reveal a secret code to outsiders. Revealing a secret code is tantamount to allowing oneself to be impersonated or observed. Presumably, policies are needed to hold someone accountable if they deliberately reveal their code. It is similar to lending a criminal your identification card so he can purchase a handgun under your name. Accountability is less clear if the secret is revealed accidentally, and this must be addressed.

Section 4: Policy Reform for Electronic Commerce

Private sector solutions are not enough to make an effective electronic commerce system a reality. Government leadership is essential.

Section 4.1: Accreditation of Commercial Notaries and Verifiers

Trustworthy commercial verifiers and notaries are needed. Some governments may simply create them. The services could be provided by a government agency, as postal and telecommunications services are in many nations. Governments will also create these services through contract with a private company, as the Canadian government did to create a national certificate authority. However, as was demonstrated in the telecommunications sector, private-sector notaries and verifiers would be more efficient than government agencies at adapting to rapidly changing technology and business conditions. Commercial competition also enhances privacy, because it allows customers to spread knowledge of their activities across multiple independent entities. Thus, like notary publics, banks, and bail bondsmen, verifiers and notaries could be private commercial entities that play a crucial part of the nation's financial infrastructure, and its law enforcement.

Government has an important role to play before commercial companies can meet this need. How does anyone know that services provided by a commercial company are dependable? Some believe that government should not interfere; companies that provide good services will gain a reputation for doing so. While government intervention should be minimized, when a commercial company plays a vital role in making tax laws enforceable, or keeping weapons from criminals, stronger assurances are needed. The federal government should support *voluntary* accreditation of verifiers and notaries. An accredited firm has shown that its services are adequate for use by federal government agencies, and to comply with federal laws. Other entities are likely to have confidence in a firm accredited for use by the federal government as well, but a state or private company is free to use a non-accredited firm. Congressman Bart Gordon recently introduced a bill that is consistent with this philosophy in the more limited context of digital signatures; the bill would instruct the Department of Commerce to identify which digital signature products and services are acceptable for use by government agencies. The list would be publicly available.

To obtain accreditation, a verifier or notary must prove that it uses technology with critical features. For example, a notary must show that any attempt to alter or delete a notarized record would be detectable. The system must be technically sound, secure, and highly dependable, so the chances of data ever being lost are remote. Any system that meets such requirements, regardless of the underlying technology, should be considered equivalent. In the context of electronic signatures, some state laws have favored specific technologies; such restrictions harm everyone except the firms who own the favored technology.

Accredited verifiers and notaries must also be financially secure and stable, and they must be well insured against error or bankruptcy. That gives the insurance company financial incentive to do effective oversight. It must be guaranteed that even if a notary or verifier goes out of business, the information it holds will be maintained so that notarized transactions it handled can be verified for a sufficient number of years.

Section 4.2: Defining New Crimes and Liabilities

What happens when a verifier incorrectly asserts that a given person has a good credit rating? A vendor who does not get paid as a result may hold the verifier liable in court. Some have asked legislators for protection by limiting liability for certificate authorities. Although this would facilitate the growth of this infant industry, it would also decrease deterrence to problems, which would be dangerous in the long term.

These new businesses also create new opportunities for behavior that should be illegal, but are not well addressed by current laws. What should the penalty be for a verifier that deliberately or through negligence violates the privacy of its customers? What should the penalty be for an individual that attempts to establish a false identity with a verifier? For an employee who deliberately reveals his employer's secret codes? Such practices were not anticipated when existing laws were written.

Section 4.3: Creating Auditors

New government functions are required. As described further in Section 3.5, a new corps of electronic commerce auditors must keep track of the verifiers and notaries used by every electronic commerce vendor. Moreover, these auditors must periodically audit randomly selected verifiers and notaries to insure they are operating honestly. This department of auditors should be in a federal agency, such as the Department of Commerce or Treasury. Congress should appropriate funding for this purpose.

Section 4.4: Reforming Regulations

To make use of the proposed system, commercial codes and tax codes must be modified to reflect what the new technology can and cannot do. At the federal level, Treasury Department regulations determine what does and does not constitute adequate records for an electronic commerce vendor facing a tax audit. Analogous agencies set regulation at the state and local levels. These agencies must act. Similarly, the Securities and Exchange Commission partially determines what level of record-keeping is sufficient when a company reports commercial activities to its stockholders. The Justice Department can address legal considerations, such as evidentiary guidelines. These regulatory codes should allow record keeping to be electronic rather than paper-based if and only if the system employed contains safeguards like those in Section 3 which allow an auditor to detect when records are either inaccurate or incomplete.

Each federal agency can and should develop regulations regarding transaction records and credentials. States would do the same, raising inevitable battles about the extent to which federal law should preempt state laws. To the extent possible, common requirements should be imposed nationwide for diverse purposes and agencies, which will require leadership from Congress or the White House. For example, Congress passed a law in 1998 introduced by Congressman Anna Eshoo and Senator Spencer Abraham that directed the federal government to begin developing a strategy for accepting electronic signatures. This may be the first step towards the development of broader electronic commerce policies.

Section 4.5: Preventing Sales to Inappropriate Parties

Once licensed notaries and verifiers exist, new restrictions can be imposed on the distribution of some material. For example, Congress can prohibit gun sales via electronic commerce to those with criminal records, and online gambling services to minors, without depriving the rest of society of these services. The laws would allow electronic commerce vendors to complete such transactions if and only if they can subsequently demonstrate to an auditor that adequate credentials were presented, where credentials are adequate if they were provided through a suitable service from an accredited verifier. (Few will be audited, but all must be prepared for an audit.)

Section 4.6: Addressing Location Uncertainty in Taxation

Under current law, a vendor should collect sales tax if and only if a given customer is located in a state at the time of the transaction where the vendor is active. There are two serious problems with this policy. First, in many cases, an electronic commerce vendor has no way of knowing where the customer is located. Second, it is often trivial for the vendor to move to a state (or country) that does not charge sales tax, and customers will not even notice the difference.

The latter problem is reason to consider collecting sales tax based on the location of the customer, independent of the location of the vendor. A practical difficulty for vendors is that state and local taxes vary considerably from one location to another, both in their tax rates, and in the items that are tax exempt (food? medicine? services? news?). It can be difficult for a vendor to know what the sales tax is, even if the vendor does know where the customer is. There are roughly 30,000 tax authorities in the US, and in 1998, they adjusted sales tax rates 579 times. This approach becomes more practical if sales taxes can be *harmonized*, at least within state boundaries. (If one could harmonize sales tax nationwide, then the problem would be solved because customers would have no motivation to misstate their location, but this would be difficult to achieve politically.) Since cities often have higher taxes than rural areas within the same state, talk of harmonization leads to conflict.

Of course, the vendor still cannot be sure where the customer is (and vise versa). At minimum, each party to a transaction should state their location for inclusion in the transaction record. When using the system described in Section 3, this would deter retroactive changes.

Customers can still misstate their location from the beginning. One solution is to define location for the purpose of tax collection on static characteristics, like billing address or tax home. This could depend on where companies incorporate or build facilities, and where individuals pay income tax, vote, or obtain a driver's license. The customer would prove this information to a verifier, who could display it when needed as credentials. Thus, this policy is easy to implement, and often effective. The disadvantage is that some may choose their billing address or tax home just to evade taxes when this is possible.

Section 5: Summary

The Internet had been a useful tool for engineers and scientists for twenty-five years when Netscape released the first commercial web browser. Suddenly, the Internet became convenient for the non-technical user to access vast information resources, and usage exploded. Roughly speaking, the Internet now doubles in size every year. The same explosion will occur with electronic commerce as soon as the available tools achieve the right combination of ease of use, security, and privacy. At that time, it will be difficult to significantly change policies governing electronic commerce. Now is the time to devise policies that are both technically enforceable and economically appropriate.

Among the most pressing policy issues of electronic commerce are taxation, privacy, fraud protection, and restricted sales (such as pornography to minors and strong encryption to foreign organizations). These controversies have been debated in isolation. In each case, deficiencies in electronic commerce as it is currently implemented forces us to choose between competing social objectives, such as protecting free speech versus protecting children from pornography, or losing tax revenues versus discouraging electronic commerce.

The best solution is to address the underlying deficiencies directly. Each of these dilemmas is rooted in how information on electronic commerce transactions is derived, verified, recorded, and used. An effective solution involves the widespread creation of commercial intermediaries called *verifiers* and *notaries*. Verifiers provide reliable credentials on buyers and sellers. Notaries determine the time of transactions. They insure that transaction records are complete, and have not been altered. Dividing responsibilities for these functions among many notaries and many verifiers makes it possible to capture enough information for tax auditors and law enforcement agents to pursue illegal activities, without sacrificing privacy. Notaries and verifiers can be private self-sustaining companies. Some of the necessary services are already available on the Internet, but the complete system will not emerge without leadership from policy-makers.

The laws, regulations, and policies must catch up with the technology. Government should play a role in advancing critical standards for electronic commerce. It should help establish new institutions by developing accreditation criteria and procedures. Government should become a user of this new information infrastructure, and should amend commercial codes, tax codes, security codes, and other regulations, to encourage private businesses and individuals to use these new capabilities. Government should develop new policies with respect to taxation and restricted sales to inappropriate parties that are consistent with the new technology. And for those who try to exploit the new technology for illegal activities, policy-makers must be sure that the criminal code provides appropriate punishments.

Recommended Further Reading

N. Asokan, P. A. Janson, M. Steiner, and M. Waidner, "The State of the Art in Electronic Payment Systems," *IEEE Computer*, Vol. 30, No. 9, Sept. 1997, pp. 28-35.

D. Chaum, "Achieving Electronic Privacy," *Scientific American*, Aug. 1992, pp. 96-101.

W. J. Clinton and A. Gore, *A Framework for Global Electronic Commerce*, July 1, 1997, http://www.iitf.nist.gov/eleccomm/ecomm.htm

Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, http://www.ftc.gov/reports/privacy3/index.htm

M. Hellman, "The Mathematics of Public-Key Cryptography," *Scientific American*, Aug. 1979, pp. 146-.

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, http://www.gao.gov/new.items/gg99034t.pdf

J. P. Morgan and A. Gidari, *Survey of State Electronic and Digital Signature Legislative Initiatives*, Internet Law and Policy Forum, http://www.ilpf.org/digisig/digrep.htm

J. M. Peha, "Making Electronic Transactions Auditable and Private," *Proceedings of the Internet Society's INET-99*, June 1999, http://www.ece.cmu.edu/~peha/ecommerce.html

J. M. Peha, *Encryption Policy Issues*, 1998, http://www.ece.cmu.edu/~peha/policy.html

J. M. Peha and R. P. Strauss, "Changing Information Technology and the Fisc," *National Tax Journal*, Vol. L, No. 3, Sept. 1997, pp. 608-21, http://www.ece.cmu.edu/~peha/ecommerce.html

J. M. Peha, *A Modest Proposal for the Immodest Internet*, editorial on the 1996 Communications Decency Act, http://www.ece.cmu.edu/~peha/policy.html

M. A. Sirbu, "Credits and Debits on the Internet," *IEEE Spectrum*, Vol. 34, No. 2, Feb. 1997, pp. 23-9.