YALE
INTERNATIONAL
CENTER
FOR FINANCE

Yale ICF Working Paper No. 02-38
September 13, 2002

CONTROL AND ASSURANCE IN E-COMMERCE: PRIVACY, INTEGRITY, AND SECURITY AT e-BAY

Rong-Ruey Duh
National Taiwan University
Karim Jamal
University of Alberta at Edmonton
Shyam Sunder
Yale School of Management

This paper can be downloaded without charge from the
Social Science Research Network Electronic Paper Collection:
http://ssrn.com/abstract_id=350663

Control and Assurance In e-Commerce: Privacy, Integrity, and Security at eBay

Rong-Ruey Duh, National Taiwan University
Karim Jamal, University of Alberta
Shyam Sunder, Yale University

Please address correspondence to:

Shyam Sunder
Yale School of Management
135 Prospect Street
P.O. Box 208200
New Haven, CT 06520-8200
Phone: (203) 432-5960
Fax: (203) 432-6974

September 13, 2002

An earlier version of this paper was presented at the 2001 American Accounting Association annual meeting. The authors are grateful for the comments of the conference participants. Financial support provided to the first author by National Science Council, Republic of China is appreciated (NSC-90-2416-H-002-008).

© Copyright 2002. All rights reserved.

Control and Assurance In e-Commerce: Privacy, Integrity and Security at eBay

ABSTRACT

Concern about privacy, integrity, and security of online transactions hampers absorption of e-commerce technologies as a normal way of doing business. To gain acceptance and trust of their participants, all organizations must achieve control or expectations equilibrium—a state where participants choose to do what others expect of them. Establishing control in e-commerce requires us to expand the traditional view of internal control to encompass the activities of customers, suppliers, and other "outside" users of their electronic platforms. We present a framework for analyzing control in online auctions. Privacy, authentication, and denial-of-service attacks are three classes of risk especially prevalent in e-commerce. Using the control practices of eBay as an illustrative example, we suggest possible ways of controlling these risks. Privacy, integrity, and security of online transactions demand new types of assurance services in e-commerce. We analyze assurance services available in 2002 and discuss challenges and opportunities facing existing services such as WebTrust. The merits of developing proprietary versus industry standards, and simple operational verification of client-specific policies for e-commerce assurance services are also discussed.

Keywords: *e-commerce, Online auctions, Control, Assurance, Privacy, Integrity, Security*
JEL Classification*: L2, M4*
Data Availability: Data is available from Public Sources

Control and Assurance In e-Commerce: Privacy, Integrity and Security at eBay

1. INTRODUCTION

We present a framework for analyzing and assessing control in e-commerce by examining online auctions--one of its "killer" applications (Crockett 1999). We apply this framework to eBay—a popular consumer-oriented online auction. We identify some novel control issues, and many opportunities for new kinds of assurance services to deal with them in e-commerce. The analytical framework may be useful to online auction firms, law enforcement agencies, regulators and assurance service firms.

With sales estimated to rise from $3.3 billion in 1999 to $8.5 billion in 2001, online auctions are one of the fastest growing and most profitable segments of e-commerce (Crockett 1999). eBay is a popular online auction site where consumers and small businesses buy and sell a variety of goods in over 4,000,000 auctions per year. Gomez.com rated eBay as the top consumer-to-consumer Internet auction site for 1999 (followed by Amazon.com and Yahoo! auctions). These auctions range from small toys to consumer durables and antiques. eBay promotes itself as a community where people come to shop, get to know others, discuss issues of mutual interest, and have fun. In its mission statement, the company states that people are basically honest and trustworthy and that all buyers and sellers need to be treated with respect.

An increase in the number of consumer complaints points to a control problem in the industry, although at least some may be attributable to increased business volume. Coy (1999) in *Business Week*, Roth (2000) in *Fortune*, Dobrzynski (2000) and Guernsey (2000a) in New York Times, and Simpson (2000a, b) in *The Wall Street Journal* indicate that privacy, integrity, and security of web transactions are the most frequently voiced concerns of online auction participants. The number of complaints filed with the Federal Trade Commission (FTC) about fraud and improper behavior in online auctions has risen from 107 in 1997, to 10,700 in 1999 (Carlton and Tam 2000). In response to these complaints, the FTC started a database to gather and organize online auction complaints for legal enforcement purposes (Guidera 2000).

We examine risks posed by the activities of buyers, sellers, and the online auction operators to the integrity and security of the market and privacy of transactions. The

auction operator is expected to: (1) provide a secure trading environment, (2) assure both buyers and sellers that the auction follows a fair set of publicly announced rules, (3) detect and punish those who violate the rules, and (4) preserve various aspects of the participants' privacy. For each type of risk, we suggest possible controls, assess the practices of eBay, and explore the assurance services that may help mitigate the risks.

Section 2 provides an overview of the online auction industry. Section 3 provides a framework for analyzing the operations of online auction firms. Section 4 describes the services of eBay. Section 5 focuses on risks to the privacy of participants. Section 6 focuses on the integrity of the online auction and security of transactions. Section 7 illustrates the analysis of several rules using the proposed framework, and discusses the potential market for e-commerce assurance services. Section 8 discusses the implications of our framework and analysis for future research and regulation of e-commerce.

2. THE ONLINE AUCTION INDUSTRY

An auction is an allocation and price determination mechanism used to trade. For thousands of years, auctions have been used to trade non-standard items whose price is difficult to determine. For example Cassady (1967) mentions the use of auctions in ancient Babylon in 500 BC. An online auction does not require the buyers and sellers to be present at the same place and time. In early online auctions conducted by phone, bandwidth limited the amount of shared information. A web page can display auction procedures, bids and offers, product or service specifications, and graphics (Beam and Segev 1998). All auction activity (bids, offers, and payments) can occur asynchronously without the buyer and seller ever meeting each other. In mid-2000, there were about 150 online auction sites that sold merchandise to consumers. There are also numerous business-to-business auction sites, which are set up as proprietary exchanges (e.g., Freemarkets) specializing in assisting manufacturers in procuring parts through auctions.

Onsale, the first web-based auction site, opened in May 1995 as a merchant selling refurbished computers and electronic goods. Four months later, eBay opened with an alternative business model as a listing agent. It is a venue to facilitate transactions between buyers and sellers without offering, taking possession of, authenticating,

shipping, or settling the transaction for goods. Business terms are negotiated and settled directly between the buyer and the seller.

The eBay model attracted 14 times the trading volume of Onsale by August 1998 (Lucking-Reiley 1999a). Yahoo bought Onsale's auction business to form Yahoo Auctions, and Egghead bought its retail business. Trading volume of eBay has continued to grow at about 12 percent per month (Lucking-Reiley 1999a). In the summer of 1999, the trading volume of eBay was about $ 190,000,000 per month; ten times the trading volume of Yahoo Auctions. Amazon.com Auctions, a relative newcomer, trailed far behind. eBay's success induced new entrants like Amazon.com to provide both a merchant site, and a listing agent service (Amazon.com Auctions), giving rise to the possibility of conflict between the two roles of the site operator. In a survey of 142 online auctions by Lucking-Reiley (1999a), 73 percent were listing agents, 19 percent were merchant sites, and 7 percent combined both these roles.

Online auctions may be set up as English, Dutch, sealed-bid, or double auctions. The English auction seems to be the most popular format (85 percent in the Lucking-Reiley survey). In an English auction, the seller offers an item for sale and specifies a starting price. Buyers are free to submit bids, and raise them as they wish until the end of the auction, which is usually specified in advance by a clock. The highest bidder pays his bid price and gets the goods. Online auctions may allow the buyers to use a software agent to bid up to a pre-specified price in small increments. The auction operator may also send e-mail messages to inform buyers about the current status of their bids. Software agents may also be used to snipe or submit a bid at the end of the auction. Both Onsale and eBay use English auctions.

The sealed bid auction is the second most popular format used by 15 percent of the surveyed sites. Each buyer can submit only one bid, with no opportunity to revise bids as in English auctions. All bids are private, and opened simultaneously; and the goods are awarded to the highest bidder who pays either his own bid price (first price auction) or the price equal to the highest of the rejected bids (second price or Vickrey auction). The Chicago Wine Company and Timeshares International use the first price sealed bid auction while Sandafayre and Nauck's vintage records are examples of the second price sealed bid auction.

The Lucking-Reiley (1999a) survey found three instances of Dutch auctions and four instances of double auctions. A Dutch auction starts from a high price set by the seller. The price then drops by a fixed amount every minute until a buyer accepts the price. Intermodal exchanges (space on cargo containers for transoceanic shipping) and Klik-Klok (a variety of consumer items) use Dutch auctions. A double auction (as used by Fastparts, for example) is similar to the NASDAQ automated stock market where both buyers and sellers can submit bids and offers, until they match or cross each other and trigger a transaction.

When there is only one buyer and one seller, the auction becomes a bargain. Some websites (e.g., SplitTheDifference.com) provide support for online bargaining between third parties. Such websites confront similar assurance issues and are included in our discussion of broadly defined auctions.

3. A FRAMEWORK FOR RISK AND CONTROL IN ONLINE AUCTIONS

A control mechanism consists of rules, compliance monitoring, and enforcement. Rules without monitoring and enforcement are ineffective. Enforcement without rules is capricious and dictatorial. Rules define the lines between norms and violations, between approval and sanctions. Monitoring defines the chances of a violation being detected, investigated, and prosecuted. Enforcement specifies the magnitude of sanctions for being found guilty of a violation. Rules, monitoring, and enforcement are partial substitutes for one another. Excessive reliance on one (e.g., draconian punishment for the guilty) may be combined with less intrusive monitoring to yield similar results. Control systems strive for a balance among clarity of rules, intrusiveness and cost of monitoring, and severity of sanctions for violations.

Traditionally, internal control is defined as environment and policy designed by management to regulate the behavior of their subordinates (e.g., Arens and Loebbecke 1999). Segregation of duties, authorization policies, and recording and reconciliation procedures are examples of such controls. The accounting profession has sought to broaden the scope of control in the United States (COSO Report, 1994), and in Canada (COCO Report, 1995). Under this view, while the locus of control remains within the firm, it is expanded to cover higher managerial functions such as strategy (purpose),

commitment, capability, monitoring, and learning. KPMG's Business Measurement Process Model (Bell, Marrs, Solomon and Thomas 1997) implements such a broad view of risk-based auditing. Attempts by the audit profession to change corporate governance (especially the role of audit committees) also extend the notion of control to internal processes at the highest levels of management and the board of directors.

Sunder (1997, 2002) presents a comprehensive perspective on control to include rules, incentives, monitoring and enforcement used to bring the behavior of all participants in an organization in line with what other participants expect of them. Under this broader perspective, control is the equilibrium between actual behavior and mutual expectations of participants in an organization. It extends beyond managers and employees to shareholders, customers, suppliers, and other agents. A receiving department, for example, monitors transactions between suppliers and the firm, while accounts receivable and credit authorization procedures monitor interactions with customers. For a business to function smoothly, activities of all its participants must be in control in this broader sense. Participating agents are selected through their willingness to accept the firm's contract set. Employees, for example, may have been screened through tests, and suppliers may have to conform to product and process quality standards (e.g., ISO certifications) chosen by a firm. These agents may also have received guidance or training in the company practices and policies.

This broader concept of control is especially important in e-commerce. The traditional focus of control has been the internal processes of organizations, involving people who frequently have social relationships. Even buying a book across the counter or checking out groceries creates nontrivial social interactions between customers and employees. E-commerce strips transactions from their traditional social context. The scope of e-commerce is limited only by accessibility to the Internet and a shared system of remote deliveries and payments, which extend well beyond the traditional boundaries for most transactions. A framework of control for e-commerce must include transactions sans traditional social relationships.

Shared norms of social exchange play an important part in transactions. E-commerce transactions can be global, allowing participants who may not share a common set of cultural or ethical norms to reach one another through electronic platforms such as

eBay. This incompatibility has two simultaneous but opposite consequences. On one hand, shared e-commerce platforms may speed up the development of a homogenized set of global norms for commercial transactions and culture. On the other hand, as the cost of creating electronic platforms shrinks, special purpose platforms catering to preexisting social, linguistic, national, or technological groups may proliferate. We focus on the more challenging problem of specifying control processes for platforms that attract a broad and diverse group of participants.

Since online auctions involve actions by unrelated parties, the platform operator must establish control with respect to internal as well as external agents. Uncontrolled behavior of any agent could damage the reputation and affect the growth of the auction house. This is a new dimension of control problem because the auction house may know little about these traders when they start using its platform. In e-commerce applications, the number of such agents can be in the millions. Another control threat in e-commerce is the ability of platform operators to gather information about participants and their actions without the permission or even awareness of the latter. Such electronic information arrays create new risks of misuse by operators, or by others who may gain access to this data.

In online auctions, rules govern agents' behavior in registration, identity representation, listing, bidding, feedback, payment and shipment. Sellers and buyers are the primary agents in the online auction market. In addition, there are rules that govern both the operation of the auction site and the personal behavior of its employees. Table 1 shows a framework for analysis and evaluation of rules. First, a rule can be evaluated with respect to its impact on each of four classes of agents – buyers, sellers, employees, and operators. Second, Klein and O'Keefe (1999) propose that rules for web auctions should be evaluated by their contribution to three key goals of auction participants– privacy of information, integrity of the auction, and the security of the transactions. Four classes of agents and three goals constitute the twelve-cell matrix used in Table 1 to organize the analysis and evaluation of rules of an auction site.

Privacy in a market ensures that the use of information gathered by various participants in the market, especially operators, is confined to the purpose for which the auction participants release it, i.e., to complete the transaction at hand. Treatment of this information as a byproduct of market operation for any other purpose carries the risk of

violating privacy, unless explicit permission is granted by the auction participants. The operator should also make sure that its employees do not exploit any privileged access to such information for personal advantage. The privacy criterion evaluates the rules of the market from this point of view.

Integrity ensures that buyers intend to, can, and do pay for what they have committed to buy in an appropriate and timely manner. It may also be necessary to prevent proscribed forms of bidding behavior, registration and identification. Similarly, it is necessary to ensure that the sellers deliver goods of promised characteristics within the agreed upon period of time after the receipt of payment. It may be necessary to prevent fraudulent or phantom sales where the seller has no ability or intention of ever delivering the goods being auctioned. Maintaining the integrity of the market requires that the operators actually enforce the rules of the auction without bias. This definition of integrity is similar to the definitions of the terms "contract" and "performance" in the legal literature (Black 1976).

Security of markets means protecting the transaction process and records against malfeasance by the participants or third party interlopers. A secure market has control processes to authenticate agents, control access to data, and prevent unauthorized disclosure of data. Control processes are also required to prevent third parties from tampering with feedback records of auction participants.

Applicability of a rule to each cell of the two-dimensional matrix of Table 1 can be evaluated by identifying the associated risks, and specifying control processes to contain these risks. In the proposed framework, one can evaluate the market rules from the perspective of each class of agents, buyers, sellers, employees, and operators, and their goals (privacy, integrity and security). In the following section, we illustrate the use of this framework by analyzing eBay, the largest online auction site based on the most common business model (listing agent), and auction format (English auction).

[Please insert Table 1 about here]

4. THE eBAY SERVICE

Visitors can browse through eBay's website to view goods for sale. Registration is required to submit bids or to sell goods. Registered people can search through eBay's

listings by category labels or keywords. A unique identifier assigned to each item helps users find its description and auction location. Names of particular bidders or sellers, what they offer for sale, and their feedback history are also available. eBay encourages direct interaction between buyer and seller and views it as a key advantage of the Internet and the eBay experience. Bidders can access the seller's email address and contact the seller for additional information about the merchandise.

eBay auctions are English, with or without a reserve price. Sellers set a minimum price that serves as the starting bid. Higher bids supercede lower bids. At the end of the pre-specified auction period (3, 5, 7, or 10 days, 7 days by default), the highest bidder wins. A winning bid must equal or exceed any reserve price which must be specified and locked in the eBay computer before the auction opens. If the seller chooses a reserve price equal to the minimum starting price, there is, in effect, no reserve price. Buyers are notified about the existence of, but not the amount of any reserve price.

Sellers of reputable record may offer multiple identical units of an item for sale on eBay. Contrary to the standard usage in economics, eBay calls this a "Dutch" auction. The highest bidders purchase the goods at the lowest successful bid. The reserve price is not allowed in eBay's "Dutch" auctions.

After the auction, the buyer pays the seller, who ships the goods upon receiving the payment. Sellers pay a small insertion fee, less than the cost of a typical newspaper classified ad, to eBay regardless of a sale. In case of a sale, the seller also pays eBay a final value fee or commission. Buyer and seller receive the counterpart's user ID, email address, and other information. They agree to use this information only for eBay related communications, not to disclose this information to third parties, and not to use this data to create a database for other commercial use or sending spam. eBay's ability to monitor compliance with these conditions is unclear.

eBay provides a venue for sellers and buyers to meet, and a mechanism to communicate and enforce its rules. It does not market, authenticate, or guarantee the merchandise; and does not suffer the consequences if the participants fail to keep their promises to pay for, or ship the goods. Operators of online auctions can achieve efficient price discovery and resource allocation within this limited role.

To maintain an orderly market, eBay has formulated and enforces its policies and rules concerning membership eligibility, fees, services, bidding and buying, listing and selling, intellectual property rights, market manipulation, uses of information about participants, access, interference, feedback, and breach of the user agreement. eBay also has policies for privacy, non-payment by buyers, etc. To mitigate against fraud, eBay established a safe harbor rule, and offers services or programs such as feedback forum, escrow, insurance and ID validation.

5. INFORMATION AND PRIVACY

Development of a broad consensus among industry, government regulators, international organizations such as the OECD, and privacy advocates, scholars and activists on privacy policy and legislation is still underway. Etzioni (1999), for example, proposes five governing principles that are useful for assessing a privacy regime:

1. Notice/awareness: Participants should receive notice of an entity's information practices before they divulge any personal information.
2. Choice/consent: Participants should be given options as to uses of any personal information collected from them, especially for secondary uses that are unrelated to complete the original transaction (e.g., sale of information to third parties).
3. Access/participation: A participant should have access to the information recorded about him, and be able to modify any inaccurate or incomplete data through a specified process.
4. Integrity/security: Collectors must take reasonable steps to ensure data integrity, destroy untimely data and convert it into anonymous form before using it for secondary purposes.
5. Enforcement/redress: There must be a mechanism in place to enforce privacy policies.

Privacy at eBay

eBay has established a privacy policy. One way to summarize eBay's privacy policy would be to say "there is no privacy on the Internet." The company as well as the

participants can, and often do, gather considerable amount of personal information about others, and use it for activities unrelated to the eBay transactions.

eBay sellers or buyers must be over eighteen years old and have a valid email address. To buy or sell users must register with their email address, name, address, and phone number, and accept a template user agreement. To complete registration, the user specifies a password and a method of payment. Being the minimum necessary for economic transactions and their settlement, these requirements appear to be efficient.

eBay tracks the URL, browser software, and the IP address of participants. It uses "session" cookies and collects information about bidding and selling behavior of individuals as well as feedback about them from other users. If the user establishes a credit account, additional information is gathered such as billing address, and copy of a check or money order. A personal file retains messages posted on bulletin boards and correspondence with the company. Purchases from co-branded merchants are reported back to eBay. Users are free to decline cookies (opt-out) if their browsers permit.

The company reserves the right to disclose information about a person to law enforcement or other government officials, if necessary or appropriate for an investigation of fraud, intellectual property infringements or other illegal activities that may expose the company to liability. Similar disclosures can be made to the Verified Rights Owner Program (VeRO) run by eBay to assist investigations of suspected improper activity.

The company provides aggregated information about user behavior to advertisers without identifying individuals. Individuals are assigned a user ID (= their email address) so others can observe all activities of a given individual, and may even send unsolicited e-mail to a specific person or groups of people. eBay may also provide personal information to its subsidiaries or joint ventures, which, as claimed by eBay, adopt similar privacy policies. However, users who register on an eBay co-branded external service provider grant eBay permission to pass their email address back to that service provider. Such service providers may have different privacy policies that eBay neither controls nor endorses. The third party suppliers may also compete with regular eBay customers (many individuals run small businesses exclusively on eBay, see Guernsey 2000b) creating potential conflicts of interest.

eBay collects a considerable amount of private information about users. It allows itself wide latitude in selling and using that information for commercial purposes. eBay's registration process automatically sets the default to "yes" which ensures that unless the readers are fully alert in reading all the details, they would automatically, and perhaps inadvertently, agree to have their private information sold to or shared with telemarketers and to receive promotional material from eBay. The users have to manually select "no" to prevent having their information sold to telemarketers. Other websites (e.g., New York Times) also use a "yes" default for the question: Do you want to receive calls from telemarketers."

Risks to Privacy

The New York Times (Tedeschi 2000) reports that in a survey of Internet households, most Internet users cite inadequate privacy as the main reason why they do not shop online. In addition, a stunning 92 percent of online households do not trust online companies to keep their information private, no matter what they promise. A Louis Harris and Associates (1998) survey indicates that 69 percent of net users consider it to be "very important" that websites post privacy policies, and 94 percent of net users say that privacy audits by independent firms would increase their confidence in commercial websites. Accounting and other service firms appear to have an opportunity to sell online privacy assurance services.

eBay is a licensee of TRUSTe and claims to follow their requirement of notifying users of its privacy policy. The user agreement specifies that eBay has wide latitude in collecting and using information gathered about participants. Unless a person does not want to be a registered eBay user, he/she must agree with this policy. In other words, users are deprived of the choice and consent over how their personal information is used for secondary purposes unrelated to the transaction being conducted; and have little control over the use and distribution of this information. To a layperson without legal training, this policy does not seem to comply with the purported TRUSTe principles, nor with the spirit of the choice/consent principle proposed by Etzioni (1999).

A second privacy issue concerns eBay's feedback rating system intended to assist individuals develop an online trading reputation. Resnick and Zeckhauser (2001) report

that in 1999 when more than half of the parties provided feedback, it was almost always positive, predictive, and reciprocated. Sellers with better ratings gained higher volume but not price. Standifird (2001) finds that positive reputational ratings emerged as mildly influential in determining final bid price. Negative reputational ratings, however, were highly influential and detrimental. In any case, eBay has no control over the feedback generated by participants, even if it is offensive, harmful, inaccurate, or deceptive. eBay has a rigid feedback policy whereby feedback is removed only under exceptional circumstances (e.g., if the person gets a court order that finds the feedback to be slanderous, or otherwise illegal; the feedback makes reference to eBay (or the Federal Bureau of Investigation) investigations, or is part of a campaign of harassment). A trader who feels that she received unfair feedback cannot post a reply, or defend his/her reputation except through a court order.

A third privacy concern arises from the actions of trading participants who accumulate information about other participants in online auctions. eBay users agree not to use others' information except for auction-related communication. The emergence of auction aggregators (e.g., auctionwatch.com, biddersedge.com) suggests that eBay may not be able to control who gets the information, or what people do with it. Auction aggregators develop links that connect their sites to multiple auction sites. Their data mining tools enable a user to search multiple auction sites simultaneously for the best deal on a given good. It is unclear who owns the data listed on eBay's website. If the data are eBay's property, the auction aggregators are stealing private information (eBay sued biddersedge.com). However, if eBay is just the owner of a marketplace or "shopping mall" where prices are posted, then biddersedge.com is simply collecting public data as a service to its customers (as biddersedge.com asserts in its countersuit).

Privacy Assurance Services

TRUSTe and BBB Online were among the first providers of privacy assurance in e-commerce. As first movers, they may be vulnerable to traditional competitors (CA/CPA firms) who have proven reputations and expertise in the assurance business. The ability to develop high quality standards and proven reputations for independence are key attributes that could give CA/CPA firms a competitive advantage.

These two programs have similar requirements. To be eligible for a TRUSTe license, websites must comply with its principles of the privacy program (http//www.TRUSTe.com). User right to choice and consent over how their personal information is used and shared is one of these principles. Other principles concern the posting of a privacy policy, and disclosure about the collection and use of personal information, use of cookies, and third parties using cookies to collect data on the website. TRUSTe monitors its licensees' compliance with their own posted privacy policies and the TRUSTe program requirements. The oversight processes include initial and periodic website reviews, "seeding," and online community monitoring. TRUSTe also resolves privacy complaints and requires its licensees to cooperate with its reviews and inquiries.

In a sense the "TRUSTe" privacy seal gives users a false sense of comfort. The TRUSTe auditors may audit a given company's compliance with the company's own standards. Since there are no common standards, individual companies whose privacy practices vary over a wide range get to display the same TRUSTe privacy seal. eBay does not give its users a choice about how their personal information is used for secondary purposes (a clear violation of TRUSTe policies) and yet gets to display a TRUSTe seal. An exception is that personally identifiable information will be disclosed to external service providers only when users permit. But, if users do not agree, they will not be able to use the services provided by them. It suggests to us that TRUSTe's level of monitoring is not high. There is no indication that TRUSTe has ever revoked a privacy seal from any company, despite some widely publicized violations by TRUSTe participants (e.g., a recent scandal where Microsoft was found to be collecting information about customers registering windows 98 even though they had opted –out and expressly indicated they did not want to be tracked).[1]

PriceWaterhouseCoopers (PWC) was the first accounting firm to recognize the significant potential for an e-commerce privacy seal. PWC created a "PWC Privacy" seal based on a proprietary set of standards that draw on the established brand reputation for independence and integrity of PWC. PWC requires websites to comply with their standards in order to qualify for a PWC privacy seal.

[1] However, as will be discussed later, the rate of compliance by TRUSTe's clients is high in disclosing their privacy policy, use of cookies, and use of third-party cookies.

In the aftermath of the Microsoft registration scandal, E-loan, an online lending firm, hired PWC to perform a privacy audit and provide a PWC privacy seal. A visit to E-loan's website, www.eloan.com indicates the company tries hard to convince its consumers about its good privacy policies by carrying four different seals: PWC Privacy, TRUSTe Privacy, BBB Online Privacy, and PWC BetterWeb. PWC appears to be developing a reputation as a privacy assurance expert, and is able to sell its privacy seal even to companies whose financial statements are audited by its competitors. For example, the travel services subsidiary of Microsoft (www.expedia.com) has its security procedures reviewed by its regular auditor (Deloitte & Touche), but it displays a PWC privacy seal on its website. PWC once claimed to have over 200 clients for its privacy service, but in an unusual twist, claimed that many companies were afraid to display a privacy seal for fear that they will become a target of hackers. This is another distinctive feature of e-commerce, where public advertising of good controls and security also challenges hackers to break in.

In contrast to PWC's proprietary standards approach, some accounting firms joined professional associations (CICA and AICPA) to develop open industry standards and a seal called WebTrust. Again, the goal was to develop a set of standards so that a WebTrust seal indicates some minimum compliance with standards as opposed to TRUSTe where there are no fixed standards. WebTrust developers failed completely to appreciate the need for privacy assurance. An over-emphasis on security and threats from hackers (rather than privacy), and a traditional audit approach of perceiving management of e-commerce website operators as the client (Gibbins and Jamal 2000) rather than focusing on consumers concerns about management's behavior, led to WebTrust not having any privacy assurance at all. The lack of privacy assurance was one major shortcoming of WebTrust, which may explain the slow marketplace acceptance of this new assurance service.

The latest version of WebTrust (Version 3.0 – effective January 2001) allows WebTrust providers to co-brand their seals with the professional association, and to offer a WebTrust privacy assurance service. This new privacy assurance service will create a fascinating competition between PWC (first mover with proprietary standards) versus open industry standards (WebTrust privacy). Will the first mover prevail or will network

externalities (Shapiro and Varian 1999) dominate this market? It is obviously too early to predict a winner though the odds do not appear to favor WebTrust.

So far PWC has shown better foresight in understanding the privacy needs of consumers. PWC has a recognized brand name and incentive to invest in further developing its brand reputation, and it does not have to manage an industry consortium where individual firms try to splinter standards for their own benefit. Ernst & Young is marketing both WebTrust and its own CyberProcessor Certification (CPC) seal, thus potentially splintering the WebTrust market. Ernst & Young also has incentives to promote and develop brand name reputation for its proprietary product (CPC) rather than a common industry product (WebTrust). CPC allows management to choose its own assertions (like TRUSTe) and then Ernst & Young will provide a CPC seal. Ernst & Young is thus simultaneously marketing a fixed industry standard based seal (WebTrust) and a proprietary seal with no fixed standards (CPC). A further complication arises because the WebTrust seal also covers other services (e.g., business practices, security) so there is potential for consumers to confuse the WebTrust privacy seal with other WebTrust seals.

Jamal, Maier and Sunder (2002) programmed a web crawler to visit 100 high-traffic websites and record the cookies used by each site. Surveys indicated that users were worried about being tracked by cookies, particularly by third-party cookies used by online advertisers such as DoubleClick, which aggregate data from hundreds of websites to create user profiles for marketing purposes. Jamal, Maier and Sunder found that all websites with a privacy seal from TRUSTe or BBB Online had posted their privacy policy that was easy to find. These sites all disclosed their use of cookies; 88% of them explained what cookies are and what information they collect, and 56% even explained how to turn off or monitor the cookies. Almost all (97%) the sites that used third-party cookies disclosed their practices and 63% provided a link to the privacy policy of the third party or a link to opt-out of the third-party cookie. This rate of compliance is remarkably high, and significantly better than websites without a web seal.

Jamal, Maier and Sunder (2002) also sent their web crawler to 20 randomly chosen WebTrust clients and 20 randomly chosen PWC BetterWeb clients. Disclosure of these websites on cookie usage was good (85% for WebTrust, and 95% for PWC clients),

though none of their clients disclosed the presence of third-party cookies on their website. WebTrust and PWC standards do not require disclosure of third-party cookie usage, and their clients do not provide such disclosures. In summary, the high quality of privacy policies and actual disclosure practices by TRUSTe and BBB Online clients seem to suggest little room for accounting firms to develop superior privacy disclosure standards or compliance practices, although the accounting profession has expertise in setting standards and performing assurance service in "traditional" commerce.

6. INTEGRITY AND SECURITY OF ONLINE AUCTIONS

We discuss the threats o integrity (intent and ability to fulfill terms of contract) of online auctions by reviewing the more widely publicized violations. These are shill bidding, bid-siphoning, bid-shielding, refusal to pay, misrepresenting characteristics of goods offered for sale, and selling illegal or stolen items.

"Shill" bidding is the most widely reported violation in online auctions. It is the practice of sellers posing as buyers and submitting bids to drive up the price. For example, the seller may register under another alias and submit bids that appear to come from an independent buyer. On June 2, 2000, New York Times reported that the FBI was looking into the case of an attorney who admitted bidding $4,500 on a painting he had himself offered for sale. He also admitted to purchasing some items from himself on several occasions and then posted glowing feedback on what a wonderful seller he was (Tate 2000). New York Times searched eBay's records and identified 33 Internet names that repeatedly bid on one another's offerings. These individuals also posted glowing testimonials about one another on eBay's feedback system. eBay claims to have a proprietary software tool called "Shill Hunter" to identify such activity from its records. It claims to have warned two people and suspended 13 others (including the above-mentioned art seller) after its own investigations. How the "Shill Hunter" works and how effective it is has not been made public.

In bid-siphoning, a seller posts an item for sale, observes the email addresses of interested buyers, and then contacts them with intent to sell directly to avoid the auctioneer's service charges. When such a seller collects the payment but fails to deliver

the appropriate goods by the promised deadline, the buyer does not even have the recourse of reporting the rip-off through eBay's feedback system (Ray 2000).

In bid-shielding, two or more bidders (or one person with two aliases) conspire to keep other legitimate buyers from bidding. For example, a laptop computer is offered for sale and the starting bid is set at $100. One bidder may raise the bid to, say, $510, immediately followed by a very high bid, say $5,000, from the second (shill) bidder. The second bid keeps other potential buyers away. The high bidder withdraws his bid just before the end of the auction giving some excuse, and his partner gets the computer for $510 (Festa 1998). The existence of such behavior suggests that bids on eBay are not binding, and can be withdrawn by the buyer at any time during the auction. eBay could discourage bid-shielding by allowing sellers to specify a price above which bids are automatically accepted and auction terminates.

Failure of the buyers to pay is another problem. Since eBay conducts no credit checks, a person can bid any amount of money on any item, even without the means or intent to pay for them.

Sellers are often accused of misrepresenting the quality or features of goods listed for sale; selling fake, illegal or pirated items; and in some cases, failing to supply the item listed for sale to the winning bidder (Simpson 2000b). Some eBay users have formed a "shill posse" to expose suspected frauds on an Internet discussion group, rec.collecting.coins, by requesting the actual user name behind the screen name from eBay (Simpson 2000b). If these people can identify the individuals using multiple aliases from information provided by eBay, why doesn't eBay perform this monitoring function itself? The problem could be significantly simplified, if not eliminated, by requiring both buyers and sellers to supply their credit card numbers (as required by Amazon.com Auctions) and use their actual names before they trade.

According to their website, eBay employees are allowed to trade on eBay as long as they do so outside of their normal working hours, and must use a personal, non-company email address to conduct such business. When an employee bids on an item, (s) he is required to email a web link explaining the employee trading policy to the seller. Employees who have access to reserve prices set by sellers are forbidden from bidding on items with reserve prices. We do not have information on what mechanisms eBay uses to

enforce its employee rules, especially the possible leakage of information from eBay employees to their friends and family. Possible controls over employee behavior include making employees sign confidentiality agreements, reviewing employee-trading rules periodically with employees, monitoring trading activity of employees, and implementing controls on employees' access to auction reserve prices.

While some of the risks identified above are specifically auction related (e.g. shill-bidding), other risks (e.g., failing to pay, using stolen credit cards, improper employee behavior, misrepresenting quality or characteristics of goods) are more common, and occur in a wide variety of e-commerce websites. Many of these risks occur in traditional businesses as well, but it is easier to engage in these miss-behaviors online (e.g., use of stolen credit cards) where the risk of being embarrassed or apprehended is lower.

Mechanisms For Maintaining the Integrity of Online Auctions

A feedback forum, an insurance program, and an escrow program are the key mechanisms at eBay to deal with improper trading behavior. The feedback forum is a distinctive feature of eBay. Upon completion of a transaction, the successful buyer and seller are encouraged to record feedback about their counter parties. Each person can only be given one feedback rating for a single transaction. Every eBay user has his/her own feedback profile that is open to all users, unless he/she chooses not to do so, in which case this choice will eventually become known to the other participants. A positive feedback is given a rating of +1, a negative feedback –1, and a neutral feedback zero. An eBay user whose cumulative feedback rating falls to –4 is automatically suspended. Also, to be eligible for the eBay insurance program (described later), both seller and buyer must maintain a non-negative feedback rating. This feedback seems to be an efficient and self-enforcing mechanism for protecting security and fairness in online auctions. Since the sellers and buyers take the first stab at settling any complaints that may arise about their behavior, most users are expected to have non-negative ratings. Resnick and Zeckhauser (2001) confirmed this expectation.

The public nature of feedback records makes them a powerful enforcement tool. It also induces some competing participants to try to manipulate the feedback by getting

their confederates to post flattering feedback, or by painting their competitors in an unflattering light. Shill feedback, feedback extortion and feedback solicitation are some obvious possibilities (Dennehy 2000). For example, one con artist arranged to sell a variety of items to confederates in order to build up a highly positive feedback rating. He put the goods up for sale and at one point ran thirty auctions simultaneously. Then he decided to cash the money orders from buyers and simply disappeared with the funds (Levy and Stone 1998). eBay deals with such behavior by allowing users to file complaints or send reports to safeharbor@ebay.com. eBay takes disciplinary action, but for legal reasons, the results of the investigation may not be disclosed or shared with eBay users (Kaiser and Kaiser 2000, p.142). It would be inappropriate to disclose the identity of subjects of investigation whose behavior is not illegal. Even if eBay were convinced of the illegality of behavior of a participant, a public declaration to that effect may draw eBay itself into legal entanglements. Consequently, it tries to protect the integrity of its online auctions by keeping disclosures about the results and consequences of its investigations to a minimum. eBay does not have many direct disciplinary options other than to refer improper behavior to the police, or banish the offending party from their website. eBay also does not reimburse the defrauded buyers (Levy and Stone 1998).

To protect its participants, eBay launched insurance (through Lloyds of London) and escrow programs. The insurance program is designed to protect buyers who send the money in good faith to the seller but do not receive the goods or service. Every eligible transaction is insured for up to $200 (minus a $25 deductible). To be eligible for the insurance program, eBay users need to meet several criteria that include the good reputation of both parties, and the transaction price being greater than $25. In addition, the buyer must have registered the complaint in eBay's Fraud Reporting System within thirty days after the auction closed. The good reputation criterion reinforces the enforcement power of the feedback mechanism. It may also induce eBay users to open their personal feedback profiles to the scrutiny of others to attract transaction partners. A user not willing to disclose his/her feedback profile flashes a warning to others about the contents of the profile.

In the escrow program, the buyer makes payment through a third party that holds the funds until the buyer inspects the purchased item and decides whether to accept or

reject it. Depending on the outcome, the escrow service releases the funds to the seller or returns them to the buyer.

The eBay feedback forum seems to be an efficient but passive way of enforcing the integrity in online auctions. For traditional companies, reliance on complaints (or lawsuits) from third parties such as customers is generally not considered to be an effective feature of control systems (Arens and Loebbecke 1999). Assurance firms could assist online auction operators in devising credit screening policies, authentication policies, online payment services and even verification of assets of the people who bid for high value items. One intriguing possibility is for an assurance firm to become a certifying authority (CA) whereby individual consumers would register with the CA and provide personal information (such as credit card numbers) to the CA only. This would then make it difficult for individuals to assume an alias and engage in practices such as shill-bidding. We don't know of any instances of assurance firms serving such a role, but the possibility exists for them to be a worldwide provider of digital certification and hasten the development of a public key security infrastructure. A further difficulty for eBay involves enforcing its rules. eBay reserves the right to warn, temporarily suspend, indefinitely suspend, or terminate an account (after repeated violations) if a participant has violated the user agreement. eBay uses commercial services from Equifax and Infoglide to verify the identity of participants, and ensure that people who are suspended for misbehavior do not reregister on eBay under an alias. We have no information about the effectiveness of these verification processes. The legality of banishing people from one's business site is also not clear.

Integrity Assurance Services

WebTrust and a related service by PWC (called PWC BetterWeb) offer assurance to consumers about the integrity of transaction processing, ability of the website to provide goods and services, sales terms, and handling of customer complaints. These items provide some assurance to consumers that the website is an authentic business with some ability to provide legitimate goods or services. This is however, quite incomplete because it provides no assurance that controls are in place to monitor or prevent misbehavior by outside agents (e.g., shill-bidding). A narrow definition of control seems

to be a major detriment to the development of a comprehensive e-commerce assurance service by accounting firms.

Security of Online Auctions

Online auctions face a variety of security threats. One key threat is improper remote access to the company's data. Hackers can attempt to steal IDs, passwords and credit card numbers of online auction participants, manipulate feedback ratings of auction participants, as well as attempt to manipulate reserve prices set by sellers. The key defenses against such unauthorized access involve encryption of communications and the use of firewalls to insulate internal networks from outside attack.

We do not know the exact security configuration used by eBay. At a minimum we expect them to have the following: antivirus software, advanced capability firewalls, authentication processes (such as credit card numbers and IP addresses), a comprehensive data transfer and internal data access policy, servers stored in secure rooms with limited access security logs to monitor access to company data, storing data in encrypted form, swift posting of patches to all servers for all known security holes, data backup and disaster recovery system, periodic internal audit of control practices and a network monitoring capability.

A second key threat faced by online auctions is that of an outside attack which disrupts service. In the summer of 2000, eBay (and Yahoo) were disrupted by viruses and denial-of- service attacks. Many small businesses that do all their sales on eBay effectively shut down when eBay's site crashes (Guernsey 2000b). Disruption of service is a major business risk for eBay and leads to lawsuits from disgruntled users. Security considerations for denial-of-service attacks include antivirus software protection, need for network monitoring, a disaster recovery and business continuity plan, and an emergency response team who can protect key records and systems and delete, locate, and repel the attack. eBay may also have to have redundancy within its network infrastructure, place servers at separate physical locations on different Internet corridors (or in different geographic locations) and use caching technology to prevent denial-of-service attacks from reaching the heart of the company's network.

Security Assurance Services

The medical profession has emergency rooms to deal with pressing medical problems. The legal profession has its own equivalent of medical emergency rooms in firms like Wachtell, Lipton, Rosen & Katz. They specialize in high profile mergers and acquisitions, as well as litigation and bankruptcy (Starbuck 1993). Denial-of-service attacks may provide an opportunity for assurance firms to provide a quick security response team to deal with these attacks in real time (In personal communications from their Canadian partners we learned that Ernst & Young offers such a response team as part of its CyberProcessor Certification, though it is not mentioned in their brochures). There may be a window of opportunity for such services which may be closed by other commercial competitors (e.g., Counterplane Internet Security) or government and industry controlled services (e.g., Carnegie Mellon University's CERT or Computer Emergency Response Team) soon.

The accounting profession (CICA and AICPA) has a security product called SysTrust which offers assurance to management and the board of directors about network security, disaster recovery plans, and business continuity plans. SysTrust asks management to define their own assertions (like TRUSTe), and then the CA or CPA firm can audit compliance with management's assertions. This service is currently marketed internally to management, rather than externally to outside users of a company's website. Lack of established (fixed) standards is again a major shortcoming of SysTrust.

7. ANALYSIS OF RISKS AND CONTROL: AN EXAMPLE

In addition to providing insights into the development of assurance services for e-commerce, the framework proposed in Section 3 above can be used at various levels to specify and assess controls to maintain the privacy, integrity, and security of online auctions. We briefly illustrate the use of this framework in Table 2 at a high (global) level and Tables 3 and 4 at a more micro level, by listing some key control processes that an online auction operator could use to manage risk.

[Please insert Table 2 about here]

Table 2 shows an example of using a framework for assessing controls at a high (global) level. The top left cell, for example prompts an analyst to list and evaluate

features of the auction that affect the privacy of buyers while the bottom right cell does the same for security of the site operator. Inside the respective cells we have listed an example of a relevant factor. The ability of buyers to review, respond to, and edit the feedback posted by sellers is an example of promoting the privacy and accuracy of public information about buyers. Limiting employee access to reserve prices is an example of promoting the security of the auction with respect to employee behavior. Following this procedure, an analyst can specify and assess control processes that affect the conduct of buyers, sellers, employees, and the auction operator with respect to privacy, integrity, and security. Some of these rules may create conflicts between agents (e.g., giving buyers autonomy in posting feedback on sellers). The auction operator may have to establish some mechanism to adjudicate disputes among agents.

The framework can also be used at a more micro level to analyze the risk and control consequences of each rule of the auction site. These consequences of a rule can be entered in each of the twelve cells of Table 1. When consequences of all rules have been tabulated, entries in each cell can be evaluated to judge if each risk is satisfactorily controlled. We briefly analyze two eBay rules to illustrate this process.

Rule 1: Buyers can send feedback to eBay on seller behavior for posting on the auction website. Since the buyer's and seller's names are posted with the feedback, the rule scores negative on buyer and seller privacy, and zero on employee and operator privacy. It may encourage buyers to be overly aggressive, and sellers to be honest; therefore scoring negative on buyer integrity and positive on seller integrity. It has no security implications. See Table 3.

[Please insert Table 3 about here]

Rule 2: Seller may decide not to reveal feedback on himself/herself, in which case this decision is disclosed on the website. This rule scores positive on seller privacy but negative on seller integrity. It has no security implications. See Table 4.

[Please insert table 4 about here]

Rule 3: Buyers must provide a valid credit card number. This rule scores negative on the privacy of buyers, positive on the integrity for buyers, and positive on the integrity and security for sellers and operators. It has no employee implications. See Table 5.

[Please insert Table 5 about here]

We can analyze the consequences of all rules in this manner and then review all entries in a given cell (see Table 6). Negative entries suggest risks and positive entries suggest corrective mechanisms to help establish control in presence of risk factors. The detailed information for Integrity/Seller cell of Table 6 is shown in Table 7. The analyst can use this data to judge the balance between risks and corrective mechanisms to establish control. If the existing rules are judged not to be in balance, they may have to be modified to establish control.

[Insert Tables 6 and 7 about here]

Through such evaluations, the management may discover room for improvement in protecting privacy, integrity, and security of users. For example, if the buyers' concern about authenticity of high value objects traded online is not balanced by appropriate constraints on sellers, the auction operator may consider offering an authentication service for, say fine art or antiques. This will help anticipate and prevent problems. The unraveling of a joint venture between Sotheby's and Amazon.comAuctions (and layoffs at eBay's Butterfield unit) in the fall of 2000 suggests that concerns about authenticity of items, credit worthiness of customers, and lack of trust inhibited the expansion of their auction designs into the high end of the auction market.

This framework also provides assurance service organizations with a map to search for business opportunities in e-commerce (cf. Elliot 1998; Solomon and Peecher 1999). TRUSTe and BBBOnline, for example, offer assurance on privacy protection. This framework may help assurance organizations better segment and serve the needs of the e-commerce markets.

For government agencies such as the FTC, this framework may be useful to examine the interrelationships among the elements of control and governance mechanisms in online auctions. It may also help to develop and enforce appropriate regulatory and privacy policies.

This framework may also help scholars identify interesting research issues. For example, Lucking-Reiley (1999b) compared the efficiency of different auction formats on the Internet and found that the Dutch auction format yielded more revenue to the seller than the English auction. We need to examine the relative susceptibility of various auction formats to rule violations, and the cost of monitoring to help determine better

e-market formats. Lucking-Reiley (1999b) also points out that auction sites who charge sellers a fee (such as eBay) attract serious sellers and have a much higher success rate than auction sites who do not charge sellers a fee (such as Yahoo auctions). This suggests that the rules of the auction sites impact on the types of buyers and sellers attracted and on the success of the auction (also see Gode and Sunder 1997).

This framework raises research questions about whether a "wholesale" reputation developed by accounting firms with sophisticated financial intermediaries (such as banks and investment bankers), can be converted into a "retail" level reputation with millions of consumers. Preliminary survey results suggest the possibility exists to develop such retail reputation and brand with a large advertising budget. Questions about reputation inevitably raise the issue of what it means to be independent. Accounting firms develop a close business relationship with the management of their clients through traditional accounting and auditing work (Gibbins and Jamal 2000). Consumer suspicion about management's motives and activities in e-commerce suggest that accounting firms may have to be more vigilant to maintain the appearance as well as the fact of independence.

8. CONCLUSIONS

Control—expectational equilibrium between what participants do and what others expect of them—is essential to sustain organizations. Opacity of Internet transactions cuts common knowledge making it difficult to attain control in e-commerce.[2] Traditional approaches to accounting control focus on "internal" participants. E-Commerce business systems often bring a large number of "external" participants into direct contact with one another. For example, the online auctioneers must reckon with the possibility of their customers cheating others on the trading platform, gathering unauthorized data about them, or using the data for unrelated purposes. Establishing expectational control among all participants is a prerequisite to success, especially in e-commerce.

We propose a simple two-dimensional framework for examining the control mechanisms of online businesses. Each aspect of an online auction, for example, is examined by three criteria (privacy, security, and integrity) from the point of view of four

[2] Common knowledge (simply, knowledge of what others know) plays an important role in stability of organizations. See Sunder (1997, 2002). In absence of special efforts to remedy the problem, opacity of what software does in Internet transactions reduces common knowledge and trust, and weakens control.

classes of participants (customers, sellers, employees, and operators). This framework can be used (a) by firms to identify, compare, and fix the weaknesses in their own systems; (b) by the assurance service industry to map and develop the market for their products; (c) by regulators to develop and enforce policy on trade, privacy, and governance; and (d) by researchers to identify important open questions.

E-commerce firms face significant new risks, and parallel efforts are underway to develop proprietary and shared industry standards for assurance services in this field. The industry standard approach of WebTrust has been slow to gain market acceptance, and we do not know which approach will succeed. In a third approach, the service provider simply checks the veracity of the client claims without imposing standards of its own. Failure of TRUSTe seals to generate confidence and trust in e-commerce suggests that verification of management's claims without fixed standards is unlikely to be successful. We are not yet aware of studies of incentives, strategies, and effectiveness of these competing approaches to standardization.

Assurance service providers need to develop a "retail" level credibility with millions of individual consumers. The development of a retail reputation raises fascinating issues about brand extension from traditional markets to new e-commerce markets, and the role of independence. In addition, a variety of legal and tax issues face online auction firms. Ownership of data generated by auctions, legal responsibility for fraudulent practices by buyers and sellers, and legal enforcement of rules and regulations (Is exclusion of misbehaving traders legal?) are some examples of issues arising in e-commerce. Some accounting firms (e.g., Ernst & Young) have created affiliations with law firms and have even created a captive law firm (called Donahue, Ernst & Young) to help deal with such issues.

Electronic auction sites have not yet succeeded in attracting a significant volume of high valued items such as rare art and antiques. Cutbacks at eBay's Butterfield high end unit in the later part of the year 2000, and the collapse of a joint venture between Sotheby's and Amazon.comAuctions (Wingfield and Bensinger 2000) indicate that online auctions have difficulty penetrating the high end of the auction market. We believe that these difficulties arise from a lack of trust in the control mechanisms that govern

privacy, integrity, and security of auctions. Better design, combined with appropriate assurance services, may help the electronic auction industry grow.

REFERENCES

American Institute of Certified Public Accountants. 2000. *Exposure Draft: Web Trust Program for On-Line Privacy*. Version 3.0, August 15

Beam, C., and A. Segev. 1998. Auctions on the Internet: A field study. Working Paper 98-1032, Haas School of Business, University of Berkeley.

Bell, T., F. Marrs, I. Solomon, and H. Thomas. 1997. *Auditing Organizations through a Strategic-Systems Lens: The KPMG Business Measurement Process*. New Jersey: KPMG LLP.

Black, H.C. 1976. *Black's Law Dictionary.* Revised Fourth Edition. West Publishing: St Paul, Minnesota.

Carlton, J., and P.W. Tam. 2000. Online auctioneers face growing fraud problem. *Wall Street Journal* (Eastern Edition). May 12. p.B6.

Cassady, R. 1967. *Auctions and Auctioneering*. University of California Press, Berkeley, CA.

Canadian Institute of Chartered Accountants. 1995. *Guidance on Control*. November, Criteria of Control Board (COCO), CICA: Toronto, Canada.

Committee of Sponsoring Organizations (COSO) of the Treadway Commission. 1994. *Internal Control – Integrated Framework*. AICPA, Jersey City, NJ.

Coy, P. 2000. Going, going, gone – sucker! *Business Week*. March 20. p.124, 126.

Crockett, R.O. 1999. Going, going …richer. *Business Week*. December 13. p.EB16.

Dennehy, M. 2000. eBay motors breakdown? *AuctionWatch.com*. June 23. www.auctionwatch.com./awdaily/dailynews/june00/1-062300.html

Dobrzynski, J.H. 2000. In online auction world, hoaxes aren't easy to see. (Late New York Edition). June 2. p.A1+. *New York Times*

Elliot, R.K. 1998. Assurance services and the auditing heritage. *Auditing: A Journal of Practice and Theory (supplement)*. pp.1-7.

Etzioni, A. 1999. *The Limits of Privacy*. New York, NY: Basic Books.

Festa, P. 1998. Fraud threatens auction sites. CNET News.com, November 4. news.cnet.com/news/0-1007-200-334943.html?st.ne.fd.gif.d.

Gibbins, M., and K. Jamal. 2000. Expertise management by public accounting firms. Working Paper, University of Alberta.

Gode, D.K., and S. Sunder. 1997. What makes markets allocationally efficient? *Quarterly Journal of Economics*, Vol. CXII No. 2 (May 1997), pp. 603-630.

Guernsey, L. 2000a. A new caveat for eBay users: seller beware. *New York Times*. August 2. www.nytimes.com./library/tech/oo/o8/circuits/articles/03sell.html.

Guernsey, L. 2000b. The powers behind the auctions. *New York Times*, August 20. www.nytimes.com/library/financial/sunday/082000biz-ebay.html.

Guidera, J. 2000. FTC, states target online-auction fraud. *Wall Street Journal* (Eastern Edition). February 15. p.B8.

Harris, L. 1998. E-commerce and privacy survey. Louis Harris and Associates.www.msnbc.com/msn/427057.asp.

Jamal, K., M. Maier, and S. Sunder. 2002. Privacy in e-commerce: Reporting standards, disclosure practices and demand for audit sans government regulation. Presented at the Journal of Accounting Research Conference, University of Chicago.

Kaiser, L.F. and M. Kaiser.1999. *The Official eBay Guide*. New York: Simon & Schuster.

Klein, S. and R.M. O'Keefe.1999. The impact of the web on auctions: some empirical evidence and theoretical considerations. *International Journal of Electronic Commerce.* Spring. pp. 7-20.

Levy, S., and B. Stone. 1998. Risky bidness: You can get anything you want on the auction site eBay. But proceed with caution. *Newsweek*, December 21. www.newsweek.com:80/nw-srv/printed/us/st/tc0125_1.htm.

Lucking-Reiley, D. 1999a. Auctions on the Internet: what's being auctioned, and how? Working paper, Vanderbilt University.

Lucking-Reiley, D. 1999b.Using field experiments to test equivalence between auction formats: Magic on the Internet. *American Economic Review.* December. pp.1063-1080.

MSN.Com 2000. MSN Statement of Privacy (www.msn.com/help/legal/privacy.htm).

Porter, M.E. 2001. Strategy and the Internet. *Harvard Business Review*. March: 63 – 78.

Ray, T. 2000. Trust in big business. *Smartmoney.com*. June 27. www.smartmoney.com/smt/columns/tech/index.cfm?story=200006271.

Resnick, P., and R. Zeckhauser. 2001. Trust among strangers in Internart transactions: Empirical analysis of eBay's reputation system.Working Paper for NBER Workshop on Empirical Studies of Electronic Commerce. http://www.si.umich.edu/~presnick/papers/ebayNBER/index.html.

Roth, D. 2000. Fraud's booming in online auctions, but help is here. *Fortune*. May 29. p.276.

Shapiro, C., and Hal R. Varian. 1999. *Information Rules*. Boston, MA: Harvard Business School Press.

Simpson, G.R. 2000a. EBay site was raided by rival, FTC says. *Wall Street Journal* (Eastern Edition). January 7. p. B6.

Simpson, G.R. 2000b. Don't take wooden nickels … on eBay? ZDNet News. June 12. www.zdnet.com/zdnn/stories/news/0,4586,2586294,00.html.

Solomon, I, and M.E. Peecher. 1999. *Assurance Services: An Introduction and Applications*. South-Western College Publishing.

Standifird, S.S. 2001. Reputation and e-commerce: eBay auctions and the asymmetrical impact of positive and negative ratings. *Journal of Management* 27: 279-295.

Starbuck, W.H. 1993. Keeping a Butterfly and an Elephant in a House of Cards: The Elements of Exceptional Success.

Sunder, S. 1997. *Theory of Accounting and Control.* South-Western College Publishing.

Sunder, S. 2002. Management controls, expectations, common knowledge and culture. J*ournal of Management Accounting Research.* forthcoming.

Tate, R. 2000. The ratings game at work. Upside Today (www.upside.com/executive_briefing/3924c2c70_yahoo.html

Tedeschi, R. 2000. Sellers hire auditors to verify privacy policies and increase trust. *New York Times,* September 18. www.nytimes.com/2000/09/18/technology/18ECOMMERCE.html).

Wingfield, N., and K. Bensinger. 2000. Ebay plans layoffs at Butterfields unit, reflecting problems in high-end market. *Wall Street Journal*, November 8. http://public.wsj.com/sn/y/SB973638666385415581.html.

Table 1: A Framework for Assessing Control in Online Auctions

	Agents			
Goals	Buyers	Sellers	Employees	Operators
Privacy				
Integrity				
Security				

Table 2: High Level Control Processes

Rule 1	**Agents**			
Goals	Buyers	Sellers	Employees	Operators
Privacy	Review feedback posted by Sellers and post a response and/or edit information on file	Review feedback posted by Buyers and post a response and/or edit information on file	Sign a confidentiality agreement	Do not use auction data for secondary purposes without the participants' explicit consent
Integrity	Require Buyers to provide a credit card number and trade using their real name	Require Sellers to provide a credit card number and trade using their real name	Forbid employees from participating in auctions	Do not allow traders to withdraw bids at the last minute
Security	Assign a unique user # and password to each Buyer	Assign a unique user # and password to each Seller	Limit access to reserve prices	Encrypt data, virus detection software, and firewalls

Table 3: Micro Level Control Processes: Rule 1

Rule 1	**Agents**			
Goals	Buyers	Sellers	Employees	Operators
Privacy	-	-		
Integrity	-	+		
Security				

Table 4: Micro Level Control Processes: Rule 2

Rule 2	**Agents**			
Goals	Buyers	Sellers	Employees	Operators
Privacy		+		
Integrity		-		
Security				

Table 5: Micro Level Control Processes: Rule 3

Rule 2	**Agents**			
Goals	Buyers	Sellers	Employees	Operators
Privacy	-			
Integrity	+	+		+
Security		+		+

Table 6: Micro Level Control Processes: Rules 1-3

Rule 2	**Agents**			
Goals	Buyers	Sellers	Employees	Operators
Privacy	-,-	-,+		
Integrity	-,+	+,-,+		+
Security		+		+

Table 7: Assessment of Risks and Controls with respect to Integrity and Seller

	Sellers	
	Risks	**Controls**
Integrity		*Rule 1* promotes seller integrity by giving buyers the right to post feedback on sellers.
	Rule 2 allows seller to withhold feedback on himself from being revealed on the website.	When seller withholds feedback on himself from being revealed on the website under *Rule 2*, the decision of the seller to withhold such information itself is revealed on the site.
		Rule 3 reduces the chances that the buyer will renege on the purchase transaction.