



CRIME, FRAUD AND DECEIT ON THE INTERNET: IS THERE HYPERREALITY IN CYBERSPACE?

C. RICHARD BAKER[†]

*Department of Accounting, University of Massachusetts-Dartmouth, North
Dartmouth, MA 02747, USA*

This paper examines the questions of crime, fraud and deceit on the Internet and discusses whether such activities constitute a new type of abusive social behavior, or whether they are classic forms of capitalistic excess appearing in a new medium. Three areas of abuse are investigated, namely: securities law violations using the Internet; crime and fraud in electronic commerce; and deceitful acts by Internet companies. The advent of the Internet has allowed fraudulent schemes to be perpetuated at low cost and distributed to a wide audience. Many of these activities would not be possible without the existence of the Internet. The rapid growth of electronic commerce has been accompanied by an increased number of fraudulent acts facilitated by the unregulated nature of the medium. The rapid growth of Internet companies, often with little economic substance, and lacking traditional management and internal controls, has prompted fears of an economic collapse combined with a desire not to be left out of a potential economic bonanza. Many Internet companies engage in deceitful practices which border on fraud. This paper examines the nature of crime, fraud and deceit on the Internet and discusses the role of the state in controlling and regulating these abuses.

© 2002 Elsevier Science Ltd

Introduction

While many believe that the advent of the Internet has been a completely positive event, others feel that there is a dark side to cyberspace. This latter perspective argues that when individuals use technology excessively and eliminate direct connections with other human beings, there is a danger they will retreat from the wider world. The upshot would be that cyberspace, which is prized for its diversity and wealth of information, will foster involvement with virtual communities at the expense of real-world communities (Kaplan, 1999; Shapiro, 1999).

The Internet has the potential to enhance the power of individuals to take control of their lives. At the same time, individual power can be misused through hacking,

[†] E-mail: rbaker@umassd.edu

Received 23 June 1999; revised 18 October 2000; accepted 3 November 2000

extortion, virus spreading, sending massive e-mail spams, selling pornography, or perpetuating fraudulent securities schemes. To prevent abuses of individual power it may be necessary to curb some of the freedom that has heretofore reigned in cyberspace. The question is whether a balance can be achieved between individual freedom and the needs of the wider community. This paper focuses on crime, fraud and deceit conducted through the Internet. The paper discusses whether such activities constitute a new type of abusive social behavior or whether they are merely an extension of capitalistic excesses previously observed in other media.

The remainder of the paper is organized as follows. The first section presents a review of previous literature discussing cyberspace, fraud, hyperreality and the role of the state in controlling abuses. The second section discusses securities law violations using the Internet. The third section discusses crime and fraud in electronic commerce. The final section discusses deceitful acts on the part of Internet companies. This is followed by a discussion and conclusion.

Review of Previous Literature

Cyberspace

The term "cyberspace" was coined by William Gibson in his novel *Neuromancer* (Everett-Green, 1995; Gibson, 1984). As conceived by Gibson, cyberspace was an artificial environment providing realistic three-dimensional sensory experiences; allowing face-to-face intimacy between people in remote places. In one of Gibson's novels, a woman "meets" a mysterious financier outside a cathedral in Barcelona, Spain, though in fact she is sitting alone in an office in Brussels (Gibson, 1984).

The concept of cyberspace is now more narrowly defined as a network of linked computers, the best known of which is the Internet. The Internet was developed in the 1970s to assist US military and academic research. In 1990 the Internet was virtually unknown to the general public. By the year 2000, the Internet had millions of users throughout the world. For many of these users, cyberspace and the Internet are virtually synonymous terms. It has been predicted that the Internet will absorb radio, television, telephone, and most conventional publishing media within its embrace. Some refer to an "information super-highway" which will constitute a unified, interactive system of electronic communication. The prospect of cyberspace, with the capacity to deliver a wide range of goods and services, has prompted the formation of hundreds of dot.com companies as capitalist interests seek to exploit the potential of new medium¹ (Everett-Green, 1995; Lohr & Markoff, 1998; Hansell, 2000).

The social implications of cyberspace may overwhelm its commercial applications. Unlike radio and television which targets a passive audience, the Internet depends on users to interact with the medium and share its content. Cyberspace can encourage the formation of "virtual communities", without barriers imposed by national, ethnic, racial or geographic boundaries. Moreover, because the Internet gives everyone the tools to become a publisher, cyberspace offers a means of freeing public discourse from the control of media monopolies (Everett-Green, 1995).

On the other hand, critics argue that cyberspace, far from creating a global village, exaggerates the disparities between rich and poor². Internet users turn off their television sets only to withdraw into virtual communities existing only in an exclusive "hyperreality". Other commentators warn of the dangers to privacy. As consumers conduct more transactions in cyberspace, it becomes easier to track their spending habits, private interests, and political beliefs (Everett-Green, 1995; Agre & Rotenberg, 1997; Whittaker, 1999). Thus, the world of cyberspace may be exciting, but it is still untamed and uncharted. Some have made an analogy between cyberspace and the 19th century frontier "boom town" where there is little law and unrestrained capitalism reigns supreme (Kedrosky, 1998).

What constitutes crime, fraud and deceit on the internet?

In the realm of cyberspace, where there are few rules and regulations, what does it mean to commit a fraudulent or deceitful act³? Are deceitful acts merely excusable misdemeanors, or should they be punished as crimes? Mitchell *et al.* (1998) argue that fraud is a crime; a white-collar crime⁴. They indicate that while-collar crime is:

A contested concept which is invoked to cover abuse of position, power, drug trafficking, insider trading, fraud, poverty wages, violation of laws, theft, exploitation and concealment, resulting in financial, physical, psychological damage to some individuals and a disruption to the economic, political and social institutions and values (Mitchell *et al.*, 1998, p. 593).

Mitchell *et al.* (1998) argue that the level of white-collar crime has increased as finance capitalism and liberal economic policies have become the reigning political economic philosophy⁵, rendering it more likely that fraudulent and criminal acts will go unpunished and unprevented.

There has been little regulation of the Internet for any reason, let alone for the purpose of reducing the incidence of criminal and fraudulent acts. Mitchell *et al.* describe this resistance to regulation in the following way:

Attempts to regulate economic activity may be resisted as those who perceive their "private interests" or "freedom" to be detrimentally affected by such regulations. They strive to apply pressures, individually and collectively, upon the state to limit and dilute restrictions upon their activity. When attacking regulations, the business sector routinely ridicules and challenges the laws on the grounds that they stifle economic activity and infringe their right to privacy, etc. Subsequent deregulation may please large sections of the business sector but, in addition to risking loss of mass support for liberalization, its longer term consequence may be the undermining of confidence when the paralyzing effects of uncertainty outweigh the costs of compliance (Mitchell *et al.*, 1998, p. 592).

Is cyberspace a state of hyperreality? The role of the state

It has been argued that advanced capitalism has entered a state of hyperreality where there are few remaining connections between signs and their referents and images present themselves independently from any underlying reality (Baudrillard, 1981, 1983; McGoun, 1997; Macintosh *et al.*, 2000). Baudrillard suggests that signs and images have evolved throughout history, initially presenting themselves as

simple reflections of a basic underlying reality. This apparent one-to-one relationship between signs and referents gave way to a subsequent period in which signs and images masked and perverted a basic reality. This was followed in turn by a period in which signs and images masked the absence of a basic underlying reality. Baudrillard argues that we have now entered a state of hyperreality, where images bear no relation to any reality whatsoever (Baudrillard, 1983; McGoun, 1997).

McGoun (1997) and Macintosh *et al.* (2000) have applied Baudrillard's arguments concerning the evolution of signs and images to developments in the fields of finance and accounting. McGoun suggests that during Baudrillard's first period, money provided an accurate image of wealth. Baudrillard's second period corresponded with Marx's idea that "political economy is this immense transmutation of all values (labor, knowledge, social relations, culture, nature) into economic exchange value". (Baudrillard, 1983, p. 113; McGoun, 1997, p. 107). The third period focused on exchange for the sake of exchange, but ultimately justified by consumption, often conspicuous. In a period of hyperreality, the consumption justification is dropped and exchange proceeds merely for the sake of exchange (McGoun, 1997, p. 107).

Arguably, cyberspace is a realm of hyperreality where signs have become detached from their referents. Clear definitions of terms such as "crime", "fraud" and "deceit" may become problematic when faced with a situation of hyperreality. Mitchell *et al.*'s (1998) analysis of white-collar crime depends largely on an understanding that there is a meaningful relationship between signs, such as "crime", "fraud" and "deceit", and some underlying social reality. In this sense, crime and fraud are essentially pre-modern or modern concepts which correspond to the first two periods of the Baudrillardian paradigm.

If Baudrillard's paradigm is correct, crime, fraud and deceit in cyberspace may be difficult to control. At the same time, even if it is argued that advanced capitalism has entered into a state of hyperreality, this does not mean that there is no need to control abuse. This paper rejects the nihilistic notions implicit in the Baudrillardian paradigm in favor of seeking solutions within a modernist approach. Moreover, the role (or lack thereof) of the nation state in regulating crime, fraud and deceit in cyberspace cannot be overlooked. The apparent existence of hyperreality may result from an abrogation of the state's duties to control abuse. In a highly technological age, the state has considerable means to enable it to monitor and control electronic media. The state may be handicapped through lack of resources, or it may be handicapped through a lack of political will. Perhaps, in the name of reducing public expenditure, deregulation and cutting taxes, the state has handicapped itself. Perhaps there are powerful economic interests which seek to restrain the role for the state in regulating abuses perpetuated through the Internet. Perhaps the global nature of the Internet inhibits the formation of multi-national alliances necessary to control abusive behaviors.

The following sections of this paper will examine certain specific aspects of crime, fraud and deceit in cyberspace and inquire into the tension between the susceptibility of advanced capitalism to deceitful acts in the pursuit of wealth and the challenges faced by the state in regulating crime, fraud and deceit on the Internet.

Securities Law Violations Using the Internet

While the Internet can be a useful tool for obtaining information, it can be used to commit securities law violations. In 1998 and 1999, the US Securities and Exchange Commission cited nearly 100 companies and individuals for committing securities law violations using the Internet. Because the Internet allows information to be transmitted rapidly and inexpensively to a wide audience, it is relatively easy to send credible looking messages to many potential targets. Investors may be unable to tell the difference between legitimate and false claims. Some of the ways that securities law violations have been committed using the Internet include: e-mail spam, online investment newsletters, the pump and dump, bogus securities offerings, and risk-free offers (Wyatt, 1999; SEC, 1998).

E-mail spam

E-mail spam is similar to junk mail. Because e-mail spam is inexpensive and easy to create, persons intent on deceiving investors can use it to locate potential victims or to spread false information about a company. E-mail spam allows perpetrators of schemes to contact many more targets than through telephone calling or mass mailing. Using bulk e-mail programs, personalized messages can be sent to thousands of Internet users simultaneously (SEC, 1998). As an example of e-mail spam, the SEC cited Francis Tribble and Sloane Fitzgerald, Inc. for sending more than six million unsolicited e-mails, building false web sites, and distributing an online newsletter to promote the stock of two small, thinly traded companies. Because Tribble and Sloane failed to tell investors that the companies agreed to pay them in cash and securities, the SEC imposed a \$15 000 penalty on Tribble. The massive amount of spam distributed by Tribble and Sloane resulted in hundreds of complaints being received by the SEC's online enforcement complaint center (SEC vs. Tribble, 1998).

Online investment newsletters

Many investment newsletters have appeared in recent years on the Internet. Online newsletters offer investment information and recommend stocks. Legitimate online newsletters can help investors to gather investment information, but some are misleading, deceiving or fraudulent. Companies may pay newsletters to recommend their stocks. This practice is not illegal, but US securities laws require the newsletters to disclose who paid them, the amount, and the type of payment. If the newsletter does not disclose its relationship with the company being recommended, the newsletter has violated securities law. The newsletter may appear to be legitimate, but it earns a fee if it persuades investors to buy or sell particular stocks. Some online newsletters violate securities law by claiming to perform research on the stocks they recommend when in fact they do not. Other newsletters spread false information or promote worthless stocks. The goal is to drive up the price of the stock in order to sell at a higher price. In an example of an online newsletter violation, the SEC cited The Future Superstock (FSS), written by Jeffrey Bruss of West Chicago, Illinois, who recommended the purchase of microcap (i.e. small capitalization) stocks and predicted that they would double or triple in the months following the recommendations. In making these recommendations, FSS: (1) failed

to disclose more than \$1.6 million of compensation, in cash and stock, from the issuers; (2) failed to disclose that it had sold stock in many of the issuers shortly after the recommendations caused the prices of those stocks to rise; (3) had not performed independent research and analysis in evaluating the issuers profiled by the newsletter; and (4) lied about the success of certain prior stock picks (SEC vs. *The Future Superstock et al.*, 1998).

The pump and dump

This type of violation involves online messages that urge investors to buy a stock quickly or recommend selling before the price goes down. The sender of the e-mail message usually claims to have inside information about a company or the ability to pick stocks that will increase in price. The perpetrators of the scheme may be insiders or paid promoters who stand to gain by selling their shares after the stock price is pumped up. Once the perpetrators sell their shares and stop hyping the stock, the price usually falls and investors lose their money. This scheme is typically employed with small, thinly-traded companies because it is easier to manipulate a stock when there is relatively little information available about the company. In an example of a pump and dump, the SEC cited Charles Huttoe and 12 other defendants for secretly distributing to friends and family nearly 42 million shares of Systems of Excellence Inc., known by its ticker symbol SEXI. In this scheme, Huttoe drove up the price of SEXI shares through false press releases claiming multi-million dollar sales which did not exist, an acquisition that had not occurred, and revenue projections that had no basis in reality. He also bribed co-defendant, SGA Goldstar, to tout SEXI to subscribers to SGA Goldstar's online newsletter called Whisper Stocks. The SEC fined Huttoe \$12.5 million. Huttoe and Theodore Melcher, the author of the online newsletter, were sentenced to federal prison. In addition, four of Huttoe's colleagues pled guilty to criminal charges (SEC, 1998).

Bogus securities offerings

Shares in companies may be offered to investors directly over the Internet. Matthew Bowin solicited investors for his company, Interactive Products and Services, in a direct public offering done entirely over the Internet. Bowin raised \$190 000 from 150 investors. Instead of using the money for corporate purposes, Bowin pocketed the proceeds. The SEC sued Bowin in civil court, and the Santa Cruz, California, District Attorney's Office prosecuted him criminally. He was convicted of 54 felony counts and sentenced to jail (SEC, 1998).

The risk-free offer

This type of scheme involves e-mail messages such as: "*Exciting, Low-Risk Investment Opportunities*" inviting participation in: *wireless cable projects, prime bank securities, or eel farms*. The investment products usually do not exist. For example, IVT Systems solicited investments to finance the construction of an ethanol plant in the Dominican Republic. The Internet solicitations promised a return of 50% or more with no basis for the prediction. The solicitations included false information about contracts with well-known companies and omitted other important information about the company. In a second example, Gene Block and Renate Haag

were cited by the SEC for offering prime bank securities through the Internet, a type of security that does not exist. Block and Haag collected over \$3.5 million by promising to double investors' money in 4 months. The SEC froze their assets and prevented them from continuing their fraud. In a third example, Daniel Odulo was cited for soliciting investors for a proposed eel farm. Odulo promised investors a 20% return, claiming that the investment was low risk. He consented to a court order stopping him from breaking the securities laws (SEC, 1998).

Analysing securities law violations in cyberspace

Securities law violations using the Internet are similar to violations perpetuated prior to the advent of the Internet. The primary difference lies in the ease with which persons intent on defrauding investors can distribute their schemes to audiences throughout the world. This is the hyperreal aspect of securities law violations using the Internet. In cyberspace, the ability to authenticate claims may be reduced. As a consequence, it is difficult to regulate or prevent fraudulent schemes (Wyatt, 1999). In addition, the SEC focuses primarily on schemes perpetuated within the United States and those directed towards American citizens. The penalties imposed for securities law violations using the Internet have been relatively light, typically involving agreements not to violate securities law again or the payment of relatively light fines (SEC, 1998). Imposition of jail sentences is rare. In addition, given the limited resources and staff of regulators, it is probable that many Internet-based fraudulent schemes go undetected.

Is this a new type of abusive social behavior, or a classic form of capitalist excess transferred to a new medium? Arguably, the types of securities violations that have been pursued by the SEC to date are not really new. At the same time, the SEC only pursues violations of US laws, and in particular federal securities laws. The unregulated nature of the Internet combined with the globalization of finance capital has the potential to facilitate fraudulent schemes in cyberspace. Moreover, it is the schemes that are not defined as criminal or fraudulent that may have greatest impact. Rapid movements of capital, such as those seen in the Asian financial crises of the late 1990s, are made easier in cyberspace. Few regulatory mechanisms are in place to prevent the de-stabilization of currencies and the resulting negative impact on developing countries. As a result, the apparent hyperreality of cyberspace does have real world consequences, and not merely for victims of securities fraud.

Crime and Fraud in Electronic Commerce

The growth of the Internet has created a revolution in advanced capitalism, where dot.com companies are ubiquitous and consumers are purchasing goods and services online. Forrester Research, Inc. predicts that Internet commerce will reach \$1.3 trillion by the year 2003 (Forrester Research, 1999). The use of credit cards as the preferred currency of cyberspace is comforting to consumers because there are legal limits on the liability for unauthorized use of credit card information. At the same time, perpetrators of fraudulent schemes are constantly looking for

opportunities to obtain credit card numbers and other personal information, such as e-mail addresses, birth dates, and social security numbers, which can be sold to e-mail spam lists and in a multitude of electronic black markets. Electronic commerce is an area ripe for crime, fraud and deceitful acts.

Examples of crime and fraud in electronic commerce

Carding cash

In January 2000, a Russian hacker, operating under the nickname of Maxus, stole 300 000 credit card numbers from the supposedly secure servers of an online music store called CDuniverse. Initially Maxus threatened to offer the stolen credit card numbers for free through his web site unless CDuniverse paid him \$100 000. CDuniverse refused to pay and contacted the US FBI. Subsequently it was discovered that the extortionate demand was really an advertisement for Maxus' ability to break into secure systems and steal "virgin" credit cards. Maxus proceeded to offer the stolen credit card numbers for sale through his Maxus Credit Card Datapipe, where visitors were able to purchase the stolen numbers and use them for fraudulent purposes. Twenty-five thousand persons visited the Maxus web site before it was shut down (McWilliams, 2000).

According to AntiOnline, a company that tracks hackers and other cyber-criminals, Maxus' real name is Maxim Ivancov, a Latvian national (Vranesevich, 2000). The Maxus Credit Card Datapipe was not created to punish CDuniverse for refusing to pay the extortion money, but rather to serve as a lure for customers. Ivancov generated cash from the stolen cards in four ways: by selling them in bulk to trusted partners for \$1 each; by kick-backs from resellers; by dealing directly to small-time thieves; and by liquidating them into cash using a stolen or false merchant identification number. According to InternetNews.com (www.InternetNews.com), Maxus notified CDuniverse about the theft in December 1999, but CDuniverse did not act to stop the fraudulent use of its customer's credit card numbers until a month later (McWilliams, 2000).

The crime of "carding cash" or ringing up fraudulent charges to a merchant account has become easier through the Internet. There is an emerging electronic black market for stolen credit card numbers. "Carders" use false merchant accounts and stolen card numbers to convert goods to cash. This is done by ordering merchandise online with stolen card numbers and having the merchandise delivered to locations, such as a vacant house, after which the merchandise is pawned for cash. A brick-and-mortar merchant who passes a physical credit card through a reader is protected from fraud. Online merchants operate in a "card-not-present" environment, where they, and not the card issuer, are responsible for fraud losses. For some online retailers, losses of this nature can reach 30 percent of revenues (McWilliams, 2000).

Web site capture

In September 1999, the president of a company that produces an Internet game site for teenagers, was trying to call up his company's web site. Instead all he got was pornographic sex scenes. Every time he tried to move to a different location,

he got more pornography. It turned out that his web site had been held captive by another web site from which he could not escape without turning off his computer. Ultimately the pornographic web site was traced to Australia, and the perpetrator of the scheme was identified as a Portuguese hacker who was paid by the Australian pornographers to perform the task (Labaton, 1999).

The Internet game site was not the only web site affected by this scheme. The perpetrators hijacked the web sites of a number of well known companies and held visitors captive. The scheme involved the cloning of legitimate web pages. When the Internet users tried to reach those web pages using the Alta Vista search engine they were "page-jacked" to the pornographic site, known to its customers as Taboosisters.com, Taboohardcore.com or Tabooanimals.com. When the Internet users tried to escape those sites by clicking on their browser's "back" or "home" buttons, they were directed to other pornography sites, or "mouse-trapped". The Portuguese hacker, Carlos Pereira, was never found. The Australian company made money from the scheme in two ways. They sold advertising on the pornographic web sites. They also used the scheme to inflate the value of their domain names by increasing the viewership of those addresses through the page-jacking and mouse-trapping. They then tried to auction those domain names on an Internet auction site at an inflated value (Labaton, 1999).

Online auctions

The US National Consumer's League Internet Fraud Watch indicates that the largest number of complaints concerning fraud in electronic commerce concern on-line auctions (National Consumers League, 1999). Online auctions typically take no responsibility for the quality, the suitability, or even the existence of the merchandise offered for sale. Fraudulent sales of products using on-line auctions, such as eBay, have occurred on a regular basis. In December 1998, using a number of aliases, Jamison Piatt promised on eBay auctions that he had more than 1500 copies of the popular Furby toy ready for delivery by Christmas. In January 1999, the state of Pennsylvania's attorney general announced that Piatt agreed to reimburse 29 auction winners who never got their Furbys, and to settle any further claims within the following 3 months (Wice, 1999). In a second example, in July 1999, the US Attorney in Los Angeles announced that Robert Guest pleaded guilty to mail fraud involving a number of auctions on eBay. According to the plea agreement, Guest had offered consumer electronic equipment for sale on eBay, but failed to deliver the items after collecting payments. Prosecutors say Guest collected about \$37 000 from bidders between March and May of 1998 for which no goods were received (Reuters, 1999).

In other examples of bizarre, and perhaps fraudulent or criminal, acts there have been online offers for the sale of a young man's virginity, more than 75 human kidneys, a human liver, and several babies (Mendoza, 1999). eBay has suspended all human kidney, liver and baby dealers from their site, and referred such offers to law enforcement officials. At the same time, some auction sites tempt online shoppers with offers regarding expensive products being sold for a low price. When bidders are told they have won the auction, they are required to pay within 24 hours. Often they pay, and the goods never appear (BBC, 1999a).

Analysing crime and fraud in electronic commerce

Are crime and fraud in electronic commerce a new type of abusive social behavior, or classic forms of capitalistic excess transferred to a new medium? What appears to be the case, both in the area of securities law violations using the Internet and crime and fraud in electronic commerce, is that organizers of fraudulent schemes are able to contact large numbers of people at low cost, allowing the schemes to be perpetuated more easily. The theft of thousands of credit card numbers from a remote location might have been possible prior to the Internet, but it is the ability to sell these cards rapidly for fraudulent purposes to people all over the world that makes the crime lucrative. The capture of web sites in the United States by pornographers in Australia aided by a Portuguese hacker leads to a conclusion that we are dealing with a new type of abusive social behavior. At the same time, greed, which is the principal component of classic forms of capitalist excess, is clearly present in these acts.

The lack of face-to-face contact in cyberspace may lull users into a state of credulity with respect to suspect claims. The creation of virtual communities, and the corresponding decrease in the level of participation in real world communities, may decrease the propensity to question the reasonableness of claims or even the patent unbelievability of some of the schemes. Among perpetrators of frauds, there appears to be a reduction in impediments to such acts. The ability to deal on a faceless basis, at the click of button, with individuals throughout the world, may facilitate misleading and deceitful acts. This may be the apotheosis of advanced capitalism, where commodities are exchanged in cyberspace, often for the mere purpose of exchange or sometimes for nothing at all (McGoun, 1997).

Deceitful Acts by Internet Companies

Internet companies, with virtually no profits, few employees and little or no tangible assets may now be worth more on paper than traditional capitalist enterprises employing thousands of staff and reporting hundreds of millions of dollars of invested capital on their balance sheets⁶. Numberless would-be billionaires are struggling to become established in cyberspace. Advertising for dot.com companies assaults the senses from every direction. Ultimately many of these companies will fail. During a period of rapid growth and subsequent contraction in an industry, there are likely to be deceitful and misleading practices emerging. Even if most Internet companies are legitimate, some have no economic basis. Moreover, as with other rapidly growing industries, there may be a lack of control over systems and data, particularly when a significant portion of a company's transactions are conducted through the Internet. This is an environment ripe for fraud and deceitful acts.

Examples of deceit by internet companies*Misleading advertising revenues*

Most Internet companies are not profitable (Hansell, 1998; Kedrosky, 1998). Even Amazon.com, one of the best known Internet companies, has not earned a profit

since its inception. Because most Internet companies are not profitable, the market valuation of such companies is frequently based on a multiple of revenues rather than a multiple of earnings. The economic basis of many Internet companies lies not in the sale of products or services, but the sale of advertising. As with other forms of advertising, Internet advertising is priced based on the number of persons who view the advertisement. Internet advertising is frequently done through barter exchanges. In other words, one Internet company provides advertising for another company and vice versa. The payments are in the form of credits for advertising on the other company's web site. Revenues are produced, but there is no cash flow (Kedrosky, 1998). The increased revenues increase the purported valuation of the Internet company, but there is little basis for the increased value.

Another area in which Internet advertising revenues may be suspect lies in the measurement of the number of visitors to a web site. A web site may report that it receives one million hits (i.e. visitors), but the number of actual visitors may be as low as one percent of that number (i.e. 10 000). This is because the measurement of hits is based on factors such as the number of links and graphic images on the site. Consequently, the number of actual visitors is difficult to measure with any degree of certainty (Kedrosky, 1998).

Undisclosed kick-backs and payments

The question of deceit on the part of Internet companies came to light in early 1999, when Amazon.com was revealed to be accepting money from publishers for purportedly independent book reviews (Caruso, 1999). Since then, more examples of online deceit have been noted in the press. For example, DrKoop.com, the web site of the former US surgeon general, was revealed to be taking commissions on products and services sold through his site without disclosing such financial arrangements. Another example concerns "comparison" shopping sites for products on the Internet. Many of these sites do not disclose the methods by which their listings are determined. Many listings are based on which companies pay to be listed. Search engines deliver web addresses in response to a consumer's inquiry, but in actuality the information is delivered based on key words that are paid for by advertisers. For example, in a search for "digital camera" the following might be returned: a (paid) banner for digital cameras; a (paid) link to an online bookstore offering books on cameras; the (unpaid) search result links (Caruso, 1999).

Undisclosed invasions of privacy

In February 2000, a lawsuit was lodged in Marin County, California, against DoubleClick, Inc. for violation of privacy rights and deceptive business practices. DoubleClick is described as the foremost "ad-server" company on the Internet. Ad-servers place advertisements and other promotional messages on web sites. The advertisements are targeted to customers through the use of "cookies", which allow the ad-server to track the preferences of online consumers. It is estimated that DoubleClick has developed over 100 million data profiles of Internet users (Green, 2000). Data profiles reveal how Internet users move among web sites, what items they buy, and what sites they visit and for how long. The lawsuit against DoubleClick is based on its practice of combining data profiles with information from direct

mailers, thus allowing the specific identification of consumers. The result is that the ad-server not only knows where a person visits, and what he or she does there, but also the person's name, where they live, and their phone number (Green, 2000)⁷.

The lawsuit against DoubleClick illustrates how interests are deployed to exploit the economic potential of the Internet. While engaging in electronic commerce, on-line customers may provide information about themselves without understanding the potential for invasion of privacy that can result. Internet companies have strong incentives to gather as much information about their customers as possible. Fundamental to the business plans of many Internet companies is the claim that they can target specific groups of individuals rather than a mass audience. Advertisers are willing to pay a premium of 10% to 20% for targeted advertising. The Internet is the first medium that allows advertisers to target specific groups of customers (Green, 2000). Privacy advocates allege that Internet companies gather personal information without the consent of consumers, even though most have privacy policies which purportedly give consumers the opportunity not to provide such information. But, privacy policies can be misleading. The collection of personal data and the creation of data profiles is pervasive, and online consumers are typically not informed about the many ways that information they provide will be used (Green, 2000).

Analysing deceit by internet companies

Some would argue that the deceptive practices of Internet companies are not particularly excessive and that whatever excesses exist can be resolved through self-regulation. Others argue that there is a compelling need for regulation. A study by the Georgetown University Health Privacy Project found that even those Internet companies that have strong privacy policies often do not follow their own self-regulatory guidelines and freely share information about visitors with their business partners (Perdue, 2000). Sensing the mood of the public, there have been several laws introduced in the US Congress that would regulate the practices of Internet companies. California and New York also have bills in their legislatures. Deceitful acts on the part of Internet companies erode the notion that self-regulation is best for both the development of the Internet and for consumers.

Often overlooked in the present frenzy is the speculative nature of the growth of Internet companies. Deceptive business practices often coincide with speculative booms. As with previous booms, there may be dire economic consequences. The avalanche of Internet IPOs in 1998 and 1999 has had the hallmarks of a classic speculative bubble. As has been true of previous bubbles, it is likely that this bubble will burst, causing economic hardships for many investors. Some would say that if there are losses, this will all be a matter of course for advanced capitalism. However, a collapse in the world of cyberspace can also result in the painful destruction of real world communities.

Discussion

This paper has situated crime, fraud and deceit on the Internet within the context of debates about the nature of cyberspace and its interaction with advanced

capitalism. The examples of crime, fraud and deceit on the Internet discussed herein offer a glimpse of the relatively raw nature of capitalism and markets. Since markets and capitalism are not accompanied by strong moral guidance, crime and fraud are often inevitable. Governments and nation states have sought to intervene, but by and large they have not yet reacted forcefully to crime, fraud and deceit on the Internet. The involvement of the state is also opposed by those keen to expand the influence of "free markets" and entrepreneurial spirit. Invariably, in a world of conflicting worldviews, fraud and deceit cannot be defined in any conclusive way and the definitions are intertwined with prevailing politics⁸.

Manuel Castells has argued that global capitalism requires global regulation (Castells, 2000). He also argues that such regulation must take into account not only technological productivity and growth but also social issues that respect human values. Capitalist interests that profit from exploiting the Internet will continue to resist regulation. Access to global markets—in part by dismantling regulations and government controls—has been one of the hallmarks of advanced capitalism. Castells argues that the fragility of global capitalism is such that a new round of instability, "perhaps induced by the collapse of Internet stocks, or by a sudden panic around electronic trading networks," could trigger a stampede⁹. "There could be governments or significant segments of society opting out of global capitalism—not necessarily to build an alternative system, but just to recover some degree of control over their lives and values" (Castells, 2000). This may be the ultimate result of crime, fraud and deceit in cyberspace.

Conclusion

This paper has examined the issue of crime, fraud and deceit on the Internet, and looked at three areas with significant potential for abuse, namely: securities law violations using the Internet; crime and fraud in electronic commerce; and deceit by Internet companies. During 1998 and 1999, the SEC cited nearly 100 companies and individuals for committing securities law violations using the Internet. There have been continual reports of bizarre, fraudulent and criminal acts in electronic commerce. The rapid growth of Internet companies, often with little economic substance and without traditional management or internal controls, has led to deceitful acts which border on fraud. These three areas of abuse on the Internet have developed rapidly. It may well be that we are seeing opportunistic schemes perpetuated by clever individuals, but as Castells points out, the risks inherent in the unregulated exploitation of cyberspace are such that we need to be aware of them and take actions to reduce their potential negative impacts in the interest of fostering the beneficial use of the Internet for the betterment of society.

Notes

1. The biggest of these being the merger between America Online and Time Warner.
2. In large parts of Asia and Africa, people do not even have access to electricity, let alone computers.

3. Mitchell *et al.* (1998) define fraud as a white-collar crime. Our intent is to use Mitchell *et al.*'s definition of fraud, which equates fraud with crime. However, since crime is technically defined as an act which violates a law, the question of whether a fraudulent act constitutes a crime depends on whether the act violates a law. Not all fraudulent acts are against the law in all countries. In countries where fraud is not explicitly against the law, it may nevertheless be subject to lawsuits brought in civil courts. A deceitful act is generally immoral, but may not rise to the level of fraud under criminal or civil law. The rapid growth of Internet companies may not be deceitful or fraudulent, but the reported revenues of many Internet companies can be deceitful or even fraudulent.
4. Even though Mitchell *et al.* (1998) make reference to "white-collar" crime, crimes, frauds and deceit on the Internet may be perpetrated by persons who are dressed casually in their work environments or who are not employed at all in the traditional sense (i.e. hackers or students).
5. One might read Marx to the effect that capitalism is crime. However, we do not necessarily assert that there is a direct relationship between capitalism and crime. It can be argued that the proper functioning of capitalist society necessitates that laws be obeyed and that fraud and deceit are reduced to sufficiently low levels so that people are encouraged to participate in economic transactions.
6. At the time this paper was first written (mid-1999), this statement was true. Subsequently, there has been a decline in the prices of Internet company shares. This decline has coincided with a general decline in stock market prices. Capital market theorists would argue that it was only a matter of time before the "efficient market" would take over and Internet company shares would be "properly" priced. Nonetheless, many people lost considerable amounts of money by investing in Internet company shares when the prices of those shares were unrelated to any underlying economic fundamentals. McGoun (1997) suggests that when there is little or no relationship between share prices and underlying fundamentals that this constitutes a state of hyperreality.
7. DoubleClick has subsequently agreed not to use its technology to identify specific individuals.
8. This discussion has benefited from the observations of an anonymous reviewer.
9. The recent decline in the prices of Internet shares may be evidence of this trend.

References

- Agre, P. & Rotenberg, M., *Technology and Privacy: The New Landscape* (Cambridge, MA: The MIT Press, 1997).
- Baudrillard, J., *For a Critique of the Political Economy of the Sign* (New York: Telos Press, 1981).
- Baudrillard, J., *Simulations* (New York: Semiotexte, 1983).
- BBC, "Internet Scam File", *BBC On-line Network*, April 7, 1999a, (news.bbc.co.uk/hi/english/business/your_money/newsid_313000/313051.stm).
- BBC, "Internet Fraud to Cost UK Business Billions", *BBC On-line Network*, May 13, 1999b, (news.bbc.co.uk/hi/english/business/the_economy/newsid_342000/342644.stm).
- Caruso, D., "Online Companies Squander Public's Trust", *New York Times*, November 8, 1999, (www.nytimes.com/library/tech/99/11/biztech/articles/08digi.html).
- Castells, M., "Information Technology and Global Capitalism", in A. Giddens & W. Hutton (eds), *On the Edge: Essays on a Runaway World* (London: 2000).
- Everett-Green, R., "Computers and Information Systems, Special Report, Cyberspace" *Encyclopaedia Britannica Online* (www.eb.com:180/bol/topic?eu=122710&sctn=1#s.top).
- Forrester Research, *U.S. On-line Business Trade Will Soar To \$1.3 Trillion By 2003* (Cambridge, MA: Forrester Research, December 17, 1998), (www.forrester.com).
- Gibson, W., *Neuromancer* (New York: Ace Books, 1984).
- Green, H., "Privacy: Outrage on the Web", *Business Week On-Line*, February 14, 2000, (www.businessweek.com/2000/00_07/b3668065.htm).
- Hansell, S., "A Quiet Year in the Internet Industry", *The New York Times*, December 28, 1998, p. C1.
- Hansell, S., "America Online to Buy Time Warner for \$165 Billion", *New York Times*, January 11, 2000, (www.nytimes.com/library/financial/011100time-aol.html).
- Kaplan, C., "Writer Seeks Balance in Internet Power Shifts", *New York Times Cyber Law Journal*, June 18, 1999, (www.nytimes.com/library/tech/99/06/cyber/cyberlaw/18law.html).

- Kedrosky, P., "There's Little but Fool's Gold in the Internet Boomtown", *The Wall Street Journal*, November 23, 1998, p. A22.
- Labaton, S., "Net Sites Co-opted by Pornographers", *New York Times On-Line*, September 23, 1999 (www.nytimes.com).
- Lohr, S. & Markoff, J., "AOL Lays Out Plan for Marriage to Netscape", *New York Times On-line*, November 28, 1998, (www.nytimes.com).
- Macintosh, N., Shearer, T., Thornton, D. & Welker, M., "Accounting as Simulacrum and Hyperreality: Perspectives on Income and Capital", *Accounting, Organizations and Society*, Vol. 25, No. 1, January, 2000, pp. 13–50.
- McGoun, E., "Hyperreal Finance", *Critical Perspectives on Accounting*, Vol. 8, Nos. 1/2, February/April 1997, pp. 97–124.
- McWilliams, B., "Circle Tightens Around Online Credit Card Thief", *InternetNews.Com*, January 12, 2000, (www.internetnews.com/ec-news/article/0,1087,4_281801,00.html).
- Mendoza, M., "Bizarre and at Times Illegal Items on Online Auctions", *Associated Press*, September 10, 1999.
- Mitchell, A., Sikka, P. & Willmott, H., "Sweeping It under The Carpet: The Role of Accountancy Firms in Moneylaundering", *Accounting, Organizations and Society*, Vol. 23, No. 5/6, 1998, pp. 589–608.
- National Consumers League, *Internet Fraud Watch*, 1999, (www.nclnet.org/Internetscamfactsheet.html).
- Perdue, L., "Privacy Lawsuits Will Force VCs to Re-evaluate Profit Models", *Internet VC Watch*, February 9, 2000, (www.internetvcwatch.com/vcwatch/article/0,2112,2601_301421,00.html).
- Reuters, "Man Pleads Guilty to Defrauding Buyers on eBay", *New York Times*, July 16, 1999, (www.nytimes.com/library/tech/99/07/biztech/articles/16ebay.html).
- SEC, *Internet Fraud: How to Avoid Internet Investment Scams*, (Washington, DC: Securities and Exchange Commission, October 1998), (www.sec.gov/consumer/cyberfr.htm).
- SEC vs. John Wesley Savage *et al.*, (Washington, DC: Securities and Exchange Commission, October 1998), (www.sec.gov/enforce/litigrel/lr15954.txt).
- SEC vs. The Future Superstock *et al.*, (Washington, DC: Securities and Exchange Commission, October 1998), (www.sec.gov/enforce/litigrel/lr15958.txt).
- SEC vs. Tribble, (Washington, DC: Securities and Exchange Commission, October 1998), (www.sec.gov/enforce/litigrel/lr15959.txt).
- Shapiro, A., *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World we Know* (New York: Public Affairs, 1999).
- Vranesevich, J., "The Credit Card Hacker", *AntiOnline*, January 12, 2000, (www.anti-online.com).
- Whittaker, R., *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York: The New Press, 1999).
- Wice, N., "Furby Fraud on eBay", *Time Digital*, January 25, 1999, (cgi.pathfinder.com/time/digital/daily/0,2822,18831,00.html).
- Wyatt, E., "SEC Goes After Bogus Securities Offerings on Web", *New York Times*, May 13, 1999, (www.nytimes.com/library/tech/99/05/biztech/articles/13fraud-marketplace.html).