

Ethics and Electronic Commerce

Shona Leitch and Matthew Warren

School of Computing and Mathematics,
Deakin University, Geelong, Victoria,
Australia.

shona@deakin.edu.au

Ethics is an important element in all aspects of computing, but proves to be a real problem in the development and delivery of electronic commerce systems. There are many aspects of ethics that can affect electronic commerce systems, but perhaps the most notable and worrying to both consumers and developers is that of trust.

In a world where so much information is transmitted and shared electronically, ethical standards that in general society are applied to this medium, are often ignored or forgotten. This paper will discuss some of the ethical considerations that should be considered in electronic commerce and offer the possible solutions that can encourage developers to consider ethical considerations and prove excellence and trust to the consumer.¹

1 Introduction

On Friday the 16th of November 1999, one of the UK's largest banks and online share dealers, the Halifax Bank plc, suspended their Internet share dealing after customers were able to gain access to other people's accounts (BBC Online, 2000). Although Internet brokerages are still in their infancy and are expected to have some teething problems, it is this sort of breach of security that fails those consumers that place their trust in electronic commerce businesses. Trust that your money or shares will be secure, is only one aspect. With the huge growth in the popularity of the Internet have also come concerns over information privacy. Information Privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves (Clarke, 1997).

Privacy covers, items such as, details supplied to electronic commerce companies when, for example, making a purchase, will remain private, that will not be sold to a third party, or become part of a junk e-mail campaign.

Successful electronic commerce in one instance has (as was missing in the Halifax Bank example) a requirement and duty to ensure that personal privacy and security when logging into a website. It must try and prevent any of this information being available to unauthorised

users. Often e-mail messages are only transferred using plain text and they can very easily be scanned using specialist-filtering software. However when subscribing to an Internet Service Provider, users are unlikely to be told this by the company. Perhaps an oversight, perhaps deliberate, but surely unethical. An additional e-mail problem is the easy ability to forge sender or recipient identity.

Recent surveys that have assessed the attitude that Internet users have towards privacy on-line. They have revealed that a large number are still unsure as to the whether the transactions they place over the Internet really are secure (Scollay, 1998). And this should worry electronic commerce businesses, with so many potential online shoppers to attract to their cyber storefronts.

One of the most common and also the most lucrative ways in which electronic commerce businesses act unethically is through the use of marketing staff. Electronic commerce businesses buy information about individuals, their personal details, shopping habits and web page visitation listings. This can be done with or without the individuals knowledge by using different computing technologies.

A large number of web sites, which require users to create a member name, also ask for personal details. These details are then often sold on to companies to aid in the marketing and selling of their products. However it must be said, that particularly in Australia, there are a large number of companies, that do not partake in this type of *spam* or at least inform individuals that their data may be passed on. Cookies are one of the most commonly used computing technologies that allow the tracing of web users. They can be indicative of the individual's habits and preferences through the storage on the hard disk of all web sites visited.

The concern over Internet security, particularly with the electronic commerce has placed the computer and Internet industry in a difficult position. It would seem that self-regulation is ineffective. A study by Georgetown University found that out of the 100 most frequently visited web sites, that 94 percent of them have privacy disclosure (as do two-thirds of randomly visited sites) (Detroit Free Press, 1999).

2 Technologies

There are numbers of technologies and techniques that are now being used in an unethical manner in support of electronic commerce. We will look at some of these technologies and methods.

¹ Copyright ' 2001, Australian Computer Society, Inc. This paper appeared at the 2nd Australian Institute of Computer Ethics Conference, Canberra, Australia, December 2000, J. Weckert, Ed. Conferences in Research and Practice in Information Technology, Vol 1. Reproduction for academic, not-for profit purposes permitted provided this text is included.

2.1 Cookies

Cookies are items of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML, information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines to allow users to participate in WWW contests (but only once!), and to store shopping lists of items a user has selected while browsing through a virtual shopping mall.

However, not all cookies are equal. At first glance, the impact of cookie information access may be seen as rather limited. Once the user exits the browser, cookies acquired during the session are deleted. In addition cookies, by default, can only be accessed by the Web server and the Web page that stored the cookie in the first place (Mayer-Sch nberger, V, 1996). Thus the accuracy and the transitory nature of personal information cookies are ensured.

Cookies are based on a two-stage process (Mayer-Sch nberger, V, 1996). First the cookie is stored in the user's computer without their consent or knowledge. For example, with customizable Web search engines like My Yahoo!, a user selects categories of interest from the Web page. The Web server then creates a specific cookie, which is essentially a tagged string of text containing the user's preferences, and it transmits this cookie to the user's computer. The user's Web browser, receives the cookie and stores it in a special file called a cookie list. This happens without any notification or user consent. As a result, personal information (in this case the user's category preferences) is formatted by the Web server, transmitted, and saved by the user's computer.

During the second stage, the cookie is clandestinely and automatically transferred from the user's machine to a Web server. Whenever a user directs her Web browser to display a certain Web page from the server, the browser will, without the user's knowledge, transmit the cookie containing personal information to the Web server.

This second stage is the main area of concern. The use of cookies is become common place, browser will accept cookies unless the default settings have been changed. The reason why the use of cookies is becoming so widespread is that they can provide information. This information can be sold or used to determine user profiles.

A simple test taken by authors using their work computer (<http://www.junkbusters.com/ht/en/cookies.html>) (see figure 1) showed that a cookie was able to tell which university the authors were at, the browser the authors were using, the operating system that they were using. The cookie was saved on the authors hard disc via the university firewall and the cookie server managed to send the cookie information from the authors hard disc via the university firewall back to the test cookie server.

If a user was using an Internet Service Provider, a on-line business could try to determine who the users were with an interest in their product, or just try to send a blind email to all the users of that Internet Service provider

with the aim of reaching that individual user who visited their site.



Figure 1: Example of Cookie Information Website

2.2 Email as Commodity

Email addresses now have a financial value and they are being sold as a commodity. Some dot-com failures are resorting to selling information their customers may have thought would remain under lock and key as they scramble to find assets that can be sold to appease creditors. At least three companies (Sandoval, 2000) that have recently failed, Boo.com, Toysmart and CraftShop.com, have either sold or are trying to sell highly sought-after customer data that could include information such as phone and credit card numbers, home addresses, and even statistics on shopping habits. When money becomes an issue of survival, some businesses will do anything they can in order to survive.

2.3 Deception

Electronic commerce relies on the integrity of its data stored in digital format. Woolford (1999) emphasises the criticality of authenticity and data integrity. The effectiveness of electronic data is determined by the security associated with its systems. Transaction and stored data must have high integrity. Electronic systems form the whole in the contemporary organisation. Its internal data such as transport, accounting transaction, and client details are often transferred on open networks. Data for external consumption such as marketing materials as well as transaction interfaces are also accessible via the Internet. This makes them vulnerable to attack form anywhere (Hutchinson and Warren, 2000).

A common example of electronic deception relates to the Internet, and is known as Web spoofing. This is where an attacker sets up a fake web site to lure users in hopes of stealing their credit card numbers or other information. One hacker group set up a site called WWW.MICROS0FT.COM (see figure 2), using the number zero in place of the letter O which many users might type by mistake. Users might find themselves in a

situation that they do not notice they are using a bogus web-site and give their credit card details, etc.



Figure 2: Example of WWW.MICROSOFT.COM

The advent of the Internet has expanded the amount of data available but has also decreased the reliability of much of it. As Ulfelder (1997, p.75) says: 'There are no editors or safeguards to ensure that net information is fair or factual.' It is, in fact, a good medium for propaganda. Because 'Nobody is small on the Web' (Rapaport, 1997, p.101) opportunities exist for getting viewpoints across from many. A single person with a grudge against an organisation can weave a damaging image by setting information into a specific context. Of course, organisations can do likewise.

As deception is a conscious activity, it can be assumed that it requires some form of motive. Ford (1996) gives some insight into the types of lies and their associated motive. Whilst his analysis is related to individuals, the classification can profitably be used with organisations. Table 1 summarises Ford's findings with the author's additions for organisational motives.

Table 1 shows both sides of an organisation's motives to lie – both to protect itself, and to compromise an enemy or competitor. Organisational deceptions can be used to promote its image (the conventional public relations function), to discredit its competitors (an activity rarely admitted), or to gain advantage by other methods. This is of particular importance within the area of electronic commerce.

The act of lying is rarely admitted in organisations. The distinction between lying and such activities as advertising is also blurred. Perhaps the more neutral phrase *perception management* provides a vehicle to carry out meaningful dialogue in this area. In competitive organisational environments, it has always been a potential strategy to deceive competitors, regulators, clients, and even suppliers. But the virtual environment in

which electronic commerce is based becomes the ideal environment in which to deceive e.g. you could be dealing with Microsoft or an individual based in Columbia.

Deception techniques can be used to influence clients, the public, government agencies, and competitors. It can be used by criminals to commit fraud. It is the information management function's responsibility not only to ensure the integrity of information and data, but also to guarantee that information is collected and used to the best advantage of the organisation. In this information age, the pervasive nature of digitised data provides ample opportunities for deceivers to apply their skills. All of this issues can be directly related to electronic commerce.

Benign and salutary lies
Hysterical lies
Defensive lies
Compensatory lies
Malicious lies
Gossip
Implies lies
Love intoxication lies
Pathological lies

Table 1: Types of lies

On the other hand, organisations need to reflect on the benefits of using deception themselves. Whilst the word 'deception' is not often used in the context of advertising, or public relations because of its negative nature, this is really what these functions are. Advertising is not just informative, it is designed to change perceptions. Deception techniques can be used to influence clients, the public, government agencies, and competitors. It can be used by criminals to commit fraud. It is the information management function's responsibility not only to ensure the integrity of information and data, but also to guarantee that information is collected and used to the best advantage of the organisation. In this Information Age, the pervasive nature of digitised data provides ample opportunities for deceivers to apply their skills (Hutchinson and Warren).

3 Conclusion

For many users there is a opportunity (especially within the US Justice system) to challenge the offenders of ethical and privacy breaches in a court of law. As a user from California has recently done, claiming that DoubleClick (a web advertising firm) was unlawfully obtaining consumers private information. This is not the first case to be brought against a company such as this, and is unlikely to be the last. It seems that nothing will stop the unethical behaviour of some companies unless there is strong legal backing to the elimination of this privacy invasion. One of the major issues in relation to electronic commerce is how to attract potential customers

to particular web sites. These means that on-line companies will resort to any method in order to get users to visit their site, whether it is ethical or not.

4 References

- BBC ONLINE (2000) Online share dealing-Is it safe? http://news6.thdo.bbc.co.uk/hi/english/business/newsid_541000/541880.stm [accessed 15/08/00].
- CLARKE, R (1997) Introduction to Dataveillance and Information Privacy, and Definitions of Terms <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html> [accessed 11/08/00].
- DETROIT FREE PRESS (1999) Study finds Internet sites selling personal information <http://www.freep.com/tech/qtche28.htm> [accessed 11/08/00].
- HUTCHINSON, W. AND WARREN M.J (To be published 2001), Truth, Lies, reality and deception: an issue for Electronic Commerce, *International Journal of Technology Management*, MCB Press, UK.
- HUTCHINSON, W. AND WARREN M.J. *Nothing is Real: Deception in the Information Age*, INC (International Network Conference) 2000, Plymouth, UK, July, 2000.
- FORD, C.V. (1996) Lies! Lies!! Lies!!! The Psychology of Deceit. *American Psychiatric Press, Washington*.
- MAYER-SCHNBERGER VIKTOR (1996), Improving Computer Security on the Internet through Novel Legal Venues - Cookies for a Treat?, *Proceedings eicar '96 (European Institute for Computer Anti-Virus Research)* p.p. 155-162.
- RAPAPORT, R. (1997). PR finds a new cool tool, *Forbes*, Oct 6, 1997, p.101-108.
- SANDOVAL, G (2000). Failed dot-coms may be selling your private information *CNET News.com*, June 29, 2000.
- SCOLLAY, M (1998) 'Privacy Protection in Australia: How far have we come?', *Telecommunications Journal of Australia*, vol. 48, no. 2, pp. 7-14.
- ULFELDER, S (1997). Lies, damn lies and the Internet, *Computerworld*, **31**:28, 75-77.
- WOOLFORD, D. (1999) Electronic Commerce: It's all a matter of trust, *Computing Canada*, 25:18, 13-15.