Privacy issues of using cashless mediums of exchange over the internet

A. M. Young
School of Accounting and Law, RMIT University, Australia

Abstract

There is evidence to suggest that cashless mediums of exchange are becoming more prolific. Following on from the physical use of credit and debit cards, bills can now be simply paid by phone or via the internet by the average consumer. This paper explores the privacy issues that arise as a result of the burgeoning electronic payment system over the internet. When trading using cashless mediums of exchange, record keeping functionally replaces cash. These ubiquitous records imperil privacy. A privacy issue arises with the collection of private information, despite whether it is used or not. Authorised use by authorised parties does not necessarily mean that privacy is protected. Non authorised uses by either authorised or non authorised parties are direct threats to privacy. Protection methods such as encryption software are compromised by market forces which drive the sale of the software, making protection a moving technical target. Legislators in America have allowed this situation by making the sales legal. Legislation changes so far are not seen to be sufficient to protect privacy related to cashless mediums of exchange on the internet.
Keywords: privacy, internet, legislation, encryption.

1 Introduction

Following on from the physical use of credit and debit cards, bills can now be simply paid by phone or via the internet by the average consumer. The internet allows connected computers with protocols that allow interface with different operating software and different applications. "Although a system of networked computers is not new, the recent growth in the significance and use of internet banking has been astounding" according to Bollen [1].

WIT Transactions on Information and Communication Technologies, Vol 36, © 2006 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/IS060421

Cashless payments via the internet provide specific advantages to the user. Amongst the most important of these advantages is the convenience of payment. With cashless forms of exchange it is not necessary to carry sufficient cash for purchases, which could be large amounts which in turn could be lost or stolen. There is also no need to be physically present to pay a bill which can be conveniently paid via the internet. Credit facilities can also accompany cashless mediums of exchange so purchases and payments can be made without the need to have cash actually available at that time. Many credit cards offer up to 90 days of free credit. Also associated are reward point accumulations which can be used to redeem products or services including airline tickets. Associated with the lines of credit is the organised documentation of expenditure in monthly statements. This can be an important source of information for the preparation of taxation returns, personal budgets or an analysis of spending. That the credit can be traced to the vendor means there are security advantages.

2 Privacy issues

Privacy issues however accompany the method of payment. Cash or bartering systems protect privacy outside those involved in an exchange. Secondary recording systems are required to make the exchange subject to privacy issues. When trading using cashless mediums of exchange on the internet record keeping functionally replaces cash. These ubiquitous records imperil privacy which has been defined by Warren and Brandeis [9] as the "the right to be let alone". There is a trend towards increased information related to cashless mediums of exchange to improve control systems threatened by fraudulent activities. Cashless mediums of exchange add to the records kept about an individual and in potentially highly sensitive areas. The mere consolidated visibility affects a person's privacy whether that information is specifically used or not.

Access can be gained to private information by authorised parties such as the financial institution responsible for the payment, typically a bank or credit union, the vendor and government authorities such as the taxation office. Authorised uses of the information include a bank's use to transfer funds and record payment obligations, the vendors use for sales and accounting records and the taxation office which can trace records as a check on a party's compliance with tax law obligations.

Authorised uses, by authorised parties does not always constitute what many would consider ethical or even legal. There is a healthy distrust of government, financial institutions and big business. The fact that the uses made by such bodies are "authorised" provides little comfort for many individuals who commonly refer to "big brother" invasions of privacy.

In 2005 the International Law section's Information Services, Technology and Data Protection Committee "is beginning to address electronic privacy issues on an international scale" [6]. The chairman Jefferey Aresty says "the issue that we're all facing is that we've entered a new era where every business model is being transformed in some way because we're in a global space" [6].

3 Unauthorised uses

Unauthorised uses can also be made from authorised parties who may illegally use private information for their own purposes to perpetrate a fraud. Access is allowed to private information as the party is an authorised user but the party may directly abuse the trust placed in them. Electronic transfer of exchange over the internet raises the issue of great controversy about the cookie features in browser software which make it "possible for a web server to 'recognise' a web client and enables certain features that are useful for surfing and online commerce, such as retaining screen preferences, storing password, and creating virtual shopping carts" Riley [7]. In addition it is possible that "every Web site visited, every message sent or received, and every purchase made can be recorded in a database available to all comers for a modest fee" [8]. In May 2005 it was reported that "an internet company that provides shopping cart software to online merchants has agreed to settle Federal Trade Commission (FTC) charges that it rented personal information about merchants' customers to marketers knowing that such disclosure contradicted merchant privacy policies" [3].

Unauthorised uses by unauthorised people are also a very real threat to privacy. Tracing perpetrators can also be a difficult task despite the existence of a firewall, which is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks in addition to other security policies that are used with the programs. When an attacker breaches the firewall, it is nearly impossible for the network administrator to determine what occurred, and which systems were compromised.

An examination of the control environment surrounding cashless mediums of exchange raises issues of extortion and fraud at a level perhaps not thought of with physical mediums of exchange. The Australian Institute of Chartered Accountant's president Byram Johnston explained that simple fraud on the internet involving stolen identities and passwords to encrypted information protection on the Internet "allowed organised crime to do away with banks transferring money across national boundaries" [5]. It is possible for "an untraceable virtual currency for international criminals to be created on the Internet" [5].

Computer hackers have deployed a Trojan horse into programs that copy down passwords when internet users log onto remote computer systems through the vast network. Estimates of the amount of money lost to taxpayers each year due to fraud in the Commonwealth Government vary wildly. According to statistics collected by the internet fraud information centre the total loss in 2005 was $13,863,003, significantly higher than the $5,787,170 reportedly lost in 2004 [10]. Dempsey contributes that businesses "become more exposed through the internet and with the increase in e-commerce" [2].

4 Protection of privacy

American encryption software in the past were not only of significant quality but were also protected by governmental restrictions on their export. This protection has now been revoked making protection a moving target. Mr Gordon Eubanks, Chief Executive of Symantec stated "in this day and age, the government can't legislate access to technology", he continued stating that keeping the export bans would prove a "waste of time and money" [4].

5 Privacy legislation

In an attempt to protect privacy and the flow of personal data, the Australian federal Privacy act of 1988 authorised the implementation of the eleven principles developed by the Organisation for Economic Cooperation and Development in 1980. The 11 principle are as follows:

1 - Manner and purpose of collection of personal information
2 - Solicitation of personal information from individual concerned
3 - Solicitation of personal information generally
4 - Storage and security of personal information
5 - Information relating to records kept by record-keeper
6 - Access to records containing personal information
7 - Alteration of records containing personal information
8 - Record-keeper to check accuracy etc. of personal information before use
9 - Personal information to be used only for relevant purposes
10 - Limits on use of personal information
11 - Limits on disclosure of personal information

Guidelines to the "National Privacy Principles" where written by the Commissioner which included how information is collected, used and disclosed. The guidelines also consider the data's quality, security and openness along with how the data was accessed and corrected. Data identifiers were considered along with the anonymity of the data, transborder data flows and how sensitive information was handled. Via the Privacy Amendment (private sector) act this act was developed late in 2000 and covered the disclosure and use of personal information.

A review of the operation of the private sector provisions of the Privacy Act was undertaken with a report date of March 2005. The review was entitled "Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988". The report recommended a wider review of privacy laws in Australia. It also acknowledged that the "Privacy Act has not achieved its object of establishing a 'single comprehensive national scheme' for the protection of personal information." Issues included "ambiguity as to the regulatory intent of the private sector provisions". The review endorsed "national consistency in all privacy related legislation" and recommended that the "Australian Government should consider setting in place mechanisms to address inconsistencies that have come about, or will come about, as a result of exemptions in the Privacy Act".

Specifically recommendation 69 considers the applicability of privacy concerns to ensure "they remain relevant in the light of technological developments since the OECD principles were developed".

It should also be noted that the Privacy commission has jurisdiction over a number of other acts including VIIC of the Crimes act 1914, National health Act of 1953, Data-Matching Program (Assistance and Tax) act 1990 and the Telecommunications Act 1997.

6 Conclusion

With the compromise of technical protection and admissions of shortfalls in the existing privacy legislation, privacy over the internet related to cashless payments remains a concern.

References

[1] Bollen, R., The regulation of internet banking. *Journal of banking and finance law and practice*, Vol 12, pp. 5-17, March, 2001

[2] Dempsey, S., Here comes the cyber-crime busters. *Business Review Weekly*, pp 84, 16 February. 16, 2001.

[3] Editor. Internet service provider settles privacy charges. *Computer and internet lawyer*, Vol. 22, 5, pp. 23, 2005.

[4] Eubanks, G., US "should lift encryption bans" *Information Management & Computer Security*, Vol 4, 4, pp 39, 1996.

[5] Johnstone, B., Underground cash fears, *Information Management & Computer Security*. V5, 1 pp 35, 1997.

[6] Neil, M., Thinking globally. *ABA Journal*, Vol. 91, pp. 62, June 2005.

[7] Riley, T., Me and my electronic shadow: privacy - a rising trend, *Business Information Review*, Vol. 15, 2, pp83-91, 1998.

[8] Shapiro, C., Will E-Commerce erode liberty? *Harvard Business Review*, May-June, pp 189-196, 2000.

[9] Warren, S. & Brandeis, L., The right to privacy. *Harvard law review*, Vol. 4, pp. 193-220, 1890.

[10] www.fraud.org/2005_internet_fraud_report.pdf.