

M-COMMERCE

**WHAT IS IT?
WHAT WILL IT MEAN FOR CONSUMERS?**

Paper prepared for consideration

M-COMMERCE - WHAT IS IT, WHAT WILL IT MEAN FOR CONSUMERS?

Introduction	1
1. Purpose of this paper	1
2. Background	1
3. Definition of m-commerce	2
4. Uptake of m-commerce	2
4.1 United States.....	2
4.2 Europe.....	2
4.3 Japan	3
4.4 Australia.....	3
5. M-commerce services and applications	3
5.1 Content transactions	3
5.2 Credit transactions	3
6. Technology required to support m-commerce	4
7. Potential m-commerce operators	4
8. Broad regulatory framework for m-commerce	5
9. Case studies of m-commerce applications	7
9.1 Banking.....	7
9.2 Shopping.....	7
9.3 Instant purchasing.....	7
9.4 Point of sale transactions	7
9.5 Locational information and marketing	8
9.6 Gambling	8
9.7 Content and entertainment.....	8
10. Relationships in the m-commerce value chain	8
11. Possible billing models	10
11.1 Payment linked to mobile phone account.....	10
11.2 Linking payment to bank account	11
12. Issues associated with the introduction and uptake of m-commerce	11
12.1 Privacy	11
12.2 Security	12
12.3 Locational information	12
12.4 Liability for transactions.....	12
12.5 Relationships between service providers and consumers.....	13
12.6 Disclosures and disclaimers.....	13
12.7 Advertising and selling practices.....	13
12.8 Content.....	13
12.9 Intellectual property issues	14
12.10 Standards and competition.....	14
12.11 Provision of credit	14
12.12 Taxation.....	15
12.13 Evidence and Enforcement.....	15
12.14 Education and Awareness.....	15
13. Possible elements of a consumer protection framework for m-commerce	15
14. Building a consumer protection framework	16
15. Conclusion and invitation to comment	17

ATTACHMENT 1: Regulatory framework for m-commerce

M-COMMERCE - WHAT IS IT, WHAT WILL IT MEAN FOR CONSUMERS?

Introduction

There is a significant amount of "hype" about what sort of services and applications will be able to be delivered using mobile phones and other wireless devices. There is also a considerable amount of concern about how these new services will be regulated. Just as with the introduction of electronic commerce, and the use of the Internet, the uptake of mobile commerce, or m-commerce, services are likely to test the regulatory structures that are in place to deal with traditional transactions. While many of the potential problems that arise are likely to be covered by existing consumer protection mechanisms, new issues will undoubtedly emerge in the uptake of m-commerce services where consumers are left vulnerable to unfair marketing and selling practices.

1. Purpose of this paper

This paper provides a broad overview of what mobile commerce, known as m-commerce is, and the sorts of issues that are likely to emerge that regulators must consider to ensure that consumers will be protected in using m-commerce services and applications. It aims to provide a preliminary analysis, from a consumer perspective, of the types of problems that are likely to occur, various protection mechanisms that will be required to support the rollout of new m-commerce applications and services, and where gaps in the protective framework are likely to exist.

A number of the sections of this preliminary paper will be developed, and the options to improve protection for consumers using this technology explored in the next few months, in order to develop a more fully considered paper.

The purpose of this paper is to seek information from other jurisdictions on:

- potential consumer issues arising in the uptake of m-commerce;
- any policy analysis currently underway and options being considered; and
- support for coordinated work in this area.

2. Background

Mobile phone technology has been rapidly adopted in Australia. With prices falling, and in response to new marketing techniques, such as portraying mobile phones as a security option for young people and older people, users of mobile phones are demographically diverse.

To date, mobile phones are mostly used for voice traffic. However, SMS (Short Message Service) messaging has caught on with surprising speed, and in Australia is likely to already account for a significant proportion of revenue from some mobile subscribers.

The capacity for mobile technologies to offer advanced services is being strengthened with improved data rates and the move to broadband services. The greater bandwidth allows for mobile office -type applications and even video transmission, and, coupled with the capacity for an 'always on' connection, similar to the fixed environment, will increase take-up rates. There is a great deal of expectation that the soon to be introduced 3rd generation of mobile services will offer even greater functionality, but even with the interim 2.5 generation services, there has been a significant improvement in the capacity for mobile services to offer additional services.

Mobile phones incorporate ideal characteristics for performing electronic transactions, and have been identified as the future 'electronic wallet'. The SIM card, which is the identification card in the phone, is one of the only examples of the much-touted 'smart card' and can carry information or store value and provide secure authorisation and identification.

Given the central role that payment transactions play in both the economy and everyday life, policy-makers must ensure that there are adequate protection mechanisms for all stakeholders in the transaction process, in particular for consumers.

3. Definition of m-commerce

M-Commerce has been defined as the "use of handheld wireless devices to communicate, interact, and transact via high-speed connection to the Internet."

With the introduction of advanced phone technology, consumers of mobile devices will be able to access content and services anytime, anywhere. For example, they will be able to use wireless devices to access banking accounts and pay bills, receive stock quotes and initiate buy/sell transactions, or receive special promotions and generate orders from any place at any time.

There are a number of different types of electronic commerce that are likely to emerge:

- Business to Business - Electronic transactions that are conducted as part of trading, for example, the payment for the supply of goods between a producer and a wholesaler.
- Business to Consumer - Involves businesses selling their goods and services directly to consumers.
- Consumer to Consumer - Such as auctions and classified ad purchases.

The focus of this paper is primarily on issues that could arise in the conduct of Business to Consumer (B2C) transactions, such as shopping or paying for services using a mobile phone.

4. Uptake of m-commerce

4.1 United States

It has been estimated that the number of Internet-enabled mobile devices will exceed the number of PCs by 2003.¹ Another research centre, the Yankee Group similarly predicts that by 2004, more than 30% of all wireless users will access the Internet through mobile devices.

4.2 Europe

In Europe, where penetration levels for mobile phones has reached 30%, it is estimated that 10% of the adult population will be mobile Internet users. Dollars spent on mobile e-commerce services will rise to over \$200 billion in 2005.

KPMG predicts that the market for m-commerce in Europe alone is estimated to be worth 23 Billion (Euro). One of the key drivers of this growth is the significant uptake of wireless devices, including mobile phones and more advanced technologies such as palm pilots. These are continuing to develop with wireless computers linked with a cell phone emerging in the consumer market.

¹ Gartner Group estimates

4.3 Japan

Japan's I-mode service, released by DoCoMo in February 1999 is one example of a success story for m-commerce. With 1 million new subscribers joining each month, I-mode is now the largest Internet access platform in Japan. In addition to buying tickets, ordering books and getting the news delivered to a mobile handset, I-mode users can carry out banking transactions with up to 280 banks and securities brokers.

4.4 Australia

In the next 12 months, the market for mobile services and transactions is likely to be driven by early adopters, and it is expected that the mass consumer market will not contribute significantly to adoption until there is a variety of content and applications available.

The use of mobile phones for sending text messages has increased dramatically in recent years, and points to a significant potential market for m-commerce users. Telecommunications analyst Paul Budde estimates that 300 million text messages are sent by 11.5 million mobile phones over the three Australian mobile networks each month.²

While there are some examples of m-commerce currently being offered and piloted, it is estimated that the introduction of third generation (3G) mobile network, likely to be offered in Australia in 2003/04, will drive a development of wider variety of m-commerce applications. Operators will be looking for business models that can generate enough revenue to pay for the expense of building and deploying the new high-speed third generation networks.

5. M-commerce services and applications

5.1 Content transactions

Content transactions are those that involve the transfer of information one-way, although this can be personalised information, similar to promotional offers and information received via email that is addressed to a particular persons needs. It could include the transmission of news, sports, weather, and stock quotes. This could be done on a subscription basis, i.e. have the stock market quotes delivered to your mobile phone on an hourly basis for a minimum monthly charge, or on an individual basis, such as a consumer calling up a local tourism service to find a hotel when they have just driven into town.

Content transactions could also include 'push' transactions, where consumers are targeted with unsolicited advertising, known as spam, over their mobile phones. This could take the form of mass advertising, sent out to a range of mobile numbers at the same time, or could be more targeted to people in a specific location. The benefits of locational information will mean that, for example, a consumer walking down a major shopping strip is identified as being in the range of a particular shop, and offered a special deal should they choose to go in and purchase something.

5.2 Credit transactions

Credit transactions are normally two-way transactions that involve a payment function. Typical transactions include credit and debit card payments, shopping for music, books, and theatre tickets, and stock trading. It has been estimated in the United States that in five years, half of all day stock trades will be conducted from mobile phones.

² Paul Budde, quoted in Timson, L. 2002, SMS: all pervasive, insecure, *The Age* 26 February 2002.

The sorts of credit transactions that will be offered could include purchasing a drink from a vending machine, by paying for the drink (and the service) using a mobile phone handset, with the drink being released from the machine once payment has been approved, and the cost is added to the mobile phone bill. Other transactions that are likely to be popular amongst consumers could be more complex, and include ordering and arranging delivery of a pizza, or paying for a parking meter, including loading additional credit when the parking is about to run out, without needing to return to the car.

These services are likely to evolve, and incorporate a number of different features, and different types of technologies. While some, such as purchasing a drink from a vending machine could be an instant transaction, other transactions could include a hybrid of different technologies, and include instant technology mixed with the more traditional text messaging. It is likely that a number of different approaches will emerge as the technology evolves.

6. Technology required to support m-commerce

Wireless data services must be tailored specifically to the wireless device, and different devices will serve different markets. For example, for consumers, the most likely device will be the mobile phone, while for the high-end business user, other devices such as personal digital assistants, similar to mini-computers, with larger screens and more functionality will be necessary to support more complex applications.

Wireless devices are not competitive with wired connections in the speed, quality of presentation, or ease of use, but they are clearly superior in the delivery of immediate and localized information and services.

While 2.5 generation technologies can already support mobile commerce applications, as is evidenced with the run-away success of Japan's DoCoMo service, which offers mobile services using the Internet platform, and has been extremely successful among consumers, uptake of m-commerce has been constrained as a result of its technological limitations, including the limited user interface, the slow transmission of data, lack of global standards and, importantly, the limited applications available.

Technological progress is quickly overcoming these issues, and it is expected that adoption of m-commerce will rise. In Australia, the issue of developing billing systems has been a significant factor in slowing rollout of m-commerce services and applications.

7. Potential m-commerce operators

One group of operators that will be likely to offer m-commerce services are telecommunications operators. They already have a customer base, have the technical expertise, and the experience of handling payments, specifically micro payments. Further, these operators are continuing to examine options that will ensure that the cost of subsidised handsets is recouped.

Mobile operators can move into the financial services arena, including launching a credit card, procuring a banking licence or even buying a bank. We have already seen the development of branded credit cards for non-financial players, like the *Telstra* and *Qantas* cards, but mobile operators could take this even further, by producing both physical and virtual credit cards. The virtual card could be embedded into the mobile phone's SIM card, while the physical version could still be available in the consumer's wallet.

'Traditional' providers of financial and retail services have quickly adapted to the new electronic environment, not only in response to the large number of consumers using these services, but also as a reaction to the influx of virtual companies on the Internet, which have offered competitive services in increasingly price-sensitive markets. These operators have adopted the Internet into their more traditional distribution strategies, and provide the customer with reassurance that they are dealing with established brands who still have a shopfront that can be accessed, should a problem arise in the virtual relationship. Banks can become a mobile gateway, allowing the user of any mobile network to access their banking details and make payments.

Another option that is emerging is that a bank can become a mobile phone operator. If a bank chooses to become what has been termed as a Mobile Virtual Network Operator (MVNO), it can not only provide banking, but also provide phone services.

There are other potential operators also emerging. The mobile operator, offering competitive global services, without the cost of a physical space, is emerging. However, the issue of how these operators will engender trust from their customers is an issue that is currently being grappled with. The model that is occurring at the moment, is that new operators are establishing partnerships with existing providers.

The emergence of new players in the payments market, such as telecommunications operators and new networks may lead to payment provision via alternative markets, and introduce more competition.

8. Broad regulatory framework for m-commerce

In identifying the broad range of transactions that are likely to emerge for m-commerce and the potential operators that could become m-commerce providers, or be involved in different parts of the m-commerce value chain, it is likely that these applications and services will be subject to a broad regulatory regime that includes regulations covering telecommunications, broadcasting, advertising and the provision of finance and credit. In addition to industry specific regulation, competition policy will have significant impact on the overall regulation of m-commerce services, in particular relationships between providers, including mergers and other anti-competitive relationships that could emerge between different elements in the value chain.

From a preliminary analysis, different regimes have adopted different approaches to regulating the delivery of services that will have an impact on the protection offered to consumers in conducting m-commerce transactions.

For example, the European Union has focused on the security issues, with a legal framework to guarantee EU-wide recognition of electronic signatures, needed to ensure security of data transmitted electronically. The Electronic Signature Directive defines the requirements for electronic signature certificates and certification services, to ensure minimum levels of security and allow their free movement throughout the EU. There are now also a number of e-commerce influenced Directives, including the *e-commerce Directive*, the *Distance Marketing Directive*, and the *Digital Signatures Directive*.

In the United States, there are a number of national and state-based mechanisms that may be relevant in protecting consumers in the m-commerce environment. The Federal Government has adopted a self-regulatory approach to protecting consumers from being overwhelmed by

advertising using mobile technology. In 2001, the Wireless Advertising Association (WAA) established recommended privacy guidelines for its members based on the premise that wireless push advertising should only be sent to customers who have asked for it. The WAA also declared that wireless unsolicited advertising (spam) would serve neither the needs of consumers or the wireless industry, and that "Confirmed Opt-in" should become the de facto standard for wireless push advertising.

Some legislatures have also adopted additional protection mechanisms that will support m-commerce. California has recently started to regulate the use of mobile phones as payment devices. Any non-telecommunications charges placed on a telecommunications bill, including wireless bills, is regulated under a new Public Utilities Code rule, which applies to billing telephone companies, billing agents and vendors using billing services. The intent of the law is to protect consumers and businesses against abusive billing practices.

From July 1 2001 the Californian Public Utilities Commission has regulated the use of mobile phones as payment devices when the charge is billed to the consumer by the wireless telephone service provider.³ Under these regulations, telephone companies must provide consumers with the option to dispute a charge that they do not believe was authorised, and companies are prohibited from releasing confidential subscriber information. Billing companies are responsible for investigating specific complaints about charges.

In Australia, there is already both a federal and state suite of legislative instruments and bodies that are likely to have a role in overseeing and managing the introduction of mobile commerce. An overview of the different regulatory regimes that have been established for the telecommunications industry, the banking and credit industry and the content and information industry are outlined in an Attachment to this paper (see Attachment 1). This summary may not capture all the different structures that could be relevant, but do provide an illustration of the complexities that are likely to emerge in regulating m-commerce.

An important component of this regime will be the various self-regulatory mechanisms that have been put into place by individual industry organisations. Already, some mechanisms are being put into place to deal with emerging issues that are arising as a result of developments in the market, such as the use of mobile phones for advertising and marketing purposes. The Australian Communications Industry Forum, representing telecommunications carriers, is working on developing a code of conduct that will place obligations on those advertisers and marketers who wish to send out messages through mobile phone carriers to their subscribers. More detail of this approach is provided in the Appendix, and it provides a useful example of how industry is responding to provide some safeguards to consumers as the potential of m-commerce is realised.

The extent to which this framework is sufficient to protect the interests of consumers as they use m-commerce applications and services is as yet unknown, and will require further analysis. This will be essential to ensure that consumers remain protected, and to ensure that the full potential of m-commerce can be realised.

³ Caldwell, K. 2001, Federal Government and States to Regulate Mobile Payments, *The Public Policy Report, CommerceNet Newsletter*, Vol 3, No. 7, July 2001. www.commerce.net Accessed 16 April 2002

9. Case studies of m-commerce applications

9.1 Banking

A number of banks are already offering mobile banking services using the WAP mobile phone technology. Many banks currently deliver static account information to wireless devices, and an increasing number allow customers to transact over the mobile Internet. Almost half of Western Europe's WAP-enabled mobile banking accounts originate in Scandinavia, 22 percent in the UK and 13 percent in Germany.⁴

In Latvia, the mobile operator Tele2 has launched a service with the National Payments Centre, which allows regular payment of monthly bills using the mobile phone. The service uses banks' direct debit function. A user gets an SMS about the bill, and by sending a reply SMS, the bill is paid. In France, some mobile phones are equipped with a built-in credit-card slot that makes conducting mobile transactions accessible for the average mobile phone user.

9.2 Shopping

In England, *Virgin Mobile* customers can already browse the company's website via a mobile phone and buy wine, compact discs or appliances.

Other applications are likely to emerge, whereby consumers who are shopping in one store are able to call up a service that can compare the price for a given product across a range of other stores, so that the consumer can make an instant decision as to whether they should purchase, or go somewhere else.

As noted earlier, there is also significant potential for unsolicited commercial advertising, spam, and offering of special deals to customers. The potential for this will be even more significant as shops are able to monitor consumers who are in specific geographic locations. For example, a person walking through the Bourke Street Mall, could receive a spam SMS message from one of the shops offering a special discount should they choose to go into the shop.

9.3 Instant purchasing

Drink and potato chip vending machines, parking meters and public transport ticket dispensers are all likely to be able to offer instant purchasing using m-commerce applications. This will offer consumers the opportunity to purchase and pay for a product instantly, without the need for any intermediary, just as already occurs with these purchases with real money.

Telstra, Australia's major telecommunications provider is already exploring the opportunities, and has recently undertaken a "dial a coke" trial, where coke could be bought by dialling a number on the coke machine from a Telstra mobile.

9.4 Point of sale transactions

Rather than paying a tradesman by cheque, consumers will be able to conduct an instant transferral of funds from the mobile account to the account of the tradesman, linked to their identifying phone number.

⁴ Engel-Flehsig, S. 2001, Securing the new global economy, Mobile Commerce World. <http://www.mobilecommerceworld.com> Accessed 18 April 2002

9.5 Locational information and marketing

As a consumer, the option to register for offers related to upcoming events, information about a location that they are visiting, or anywhere, anytime access to information and services will be available. For example, a service could tell a person how to find the nearest petrol station when they are concerned about their fuel, or to compare prices of an item elsewhere in town while they are in a shop.

The provision of locational information will not be limited to 'pull' information, but will also include 'push' marketing, where consumers who are visiting or enter a particular location are provided with instant messages and information about specific services that are available in that area, or discounts. This will not necessarily be information that is requested or wanted, but could include information that is unsolicited, and is based purely on technology which will enable commercial companies to identify people who enter a vicinity.

9.6 Gambling

Over the next two years advances in technology will allow punters to watch live horse races on their cell phones while wagering in real time. Football fans for one team will be able to bet against supporters of the other sitting on the opposite side of the stadium.

There are already some examples of operators offering gambling using a mobile phone. In the U.K, consumers can place bets on horse and dog races over their phones with what is known as an E-Gambling card.

Gambling services have been predicted to be the major m-commerce application, and are a particular concern given the impulse associated with gambling. And, when there are no obvious restrictions, and the phone can act as a credit card, the concern is even greater.

9.7 Content and entertainment

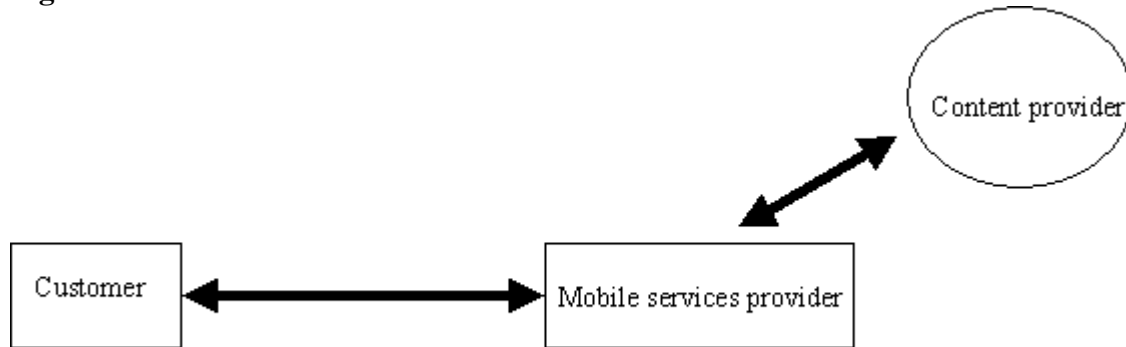
In the United States, the largest wireless phone company has announced its intention to launch a new service to allow customers to download games, entertainment and information on their phones. Using a new technology known as Binary Runtime Environment for wireless technology (BREW), consumers will be able to download applications and personalise their mobile devices through the Internet. Customers will also be able to send photo's, track expenses and access directories using the service. The billing structure envisaged for the service is that charges would be made during the downloading process and for the product, and after that time users can access the applications at any time without additional charges. Sony has been said to be developing games for the platform, however, the service will only be able to be used with BREW compatible phones, raising significant interoperability issues.

10. Relationships in the m-commerce value chain

There are likely to be a range of different relationships that will be established in different m-commerce transactions. For example, for a relatively simple transaction such as buying a can of coke, a relationship could exist between the customer and the vending machine that supplies the coke, the supplier and the telecommunications service provider, and the customer and the telecommunications service provider. These relationships become more complex when a third-party credit provider becomes involved, and additional service providers, who have emerged to specifically provide application services, such as alerting customers of special discounts and shopping bargains as they enter into a specific vicinity.

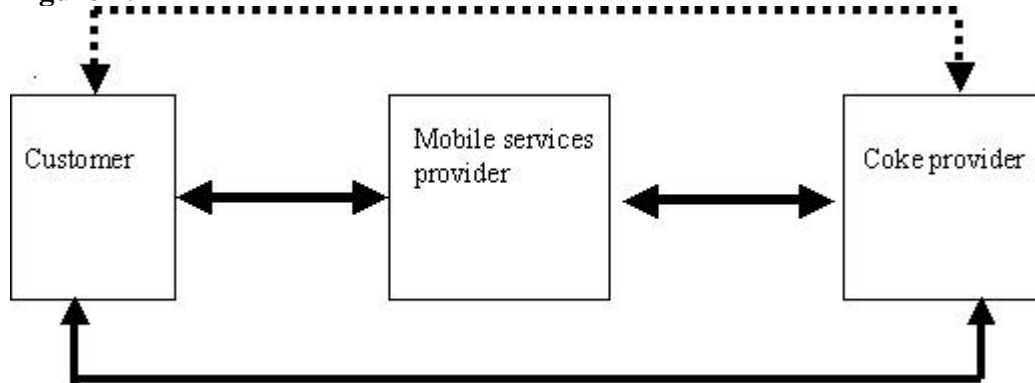
These relationships will need to be explored in some detail to determine what sorts of problems could arise in m-commerce, and what sort of protections for different elements in the value chain need to be established. In the meantime, the following set of figures will illustrate the different sorts of relationships that could emerge, involving a range of different relationships between different parties.

Figure 1:

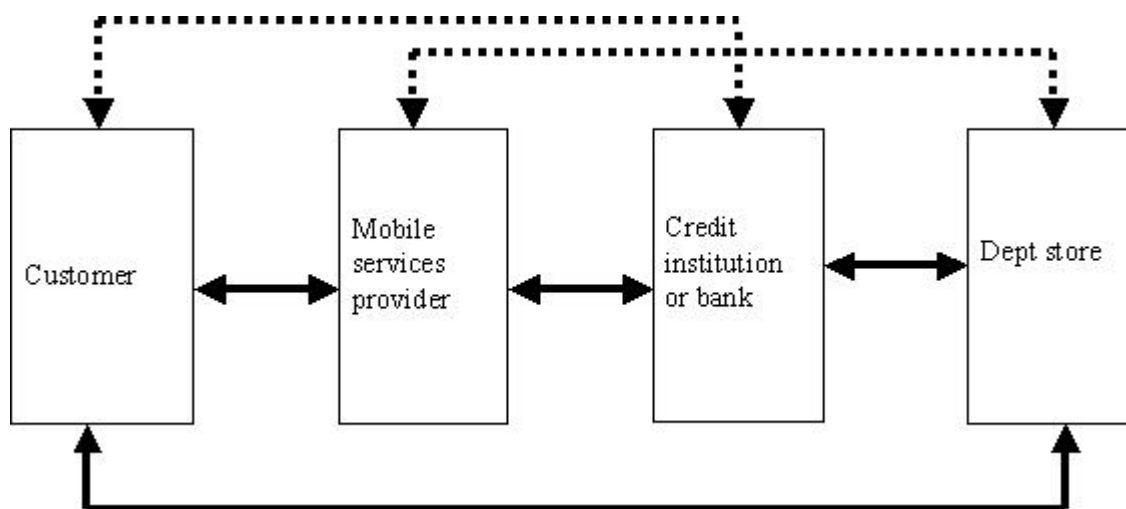


In this scenario, a relationship exists between the customer and the mobile services provider, who provides content and bills the customer for the service. The mobile services provider having a separate relationship with a content provider. While the customer is purchasing content from a third party, this relationship is transparent, and the only relationship that exists for a consumer is that with the mobile services provider.

Figure 2:



In this figure, the customer has a relationship with the mobile services provider, who charges a fee for the customer using it to purchase a coke, and adding the cost of the coke to the mobile phone bill. The mobile service provider will charge the customer a surcharge for using the service. The customer also has a relationship with the coke provider and/or the vending machine operator for the condition of the product.

Figure 3: Relationships involving financial institutions

This figure depicts the sort of relationships that a customer may have in conducting more complex m-commerce transactions. In this case, the customer might have a relationship with the mobile services provider, who provides mobile services, and enables the transaction to take place. In order to purchase products, the customer may have been required to establish a virtual bank account, which handles the transactions that the customers make, and payments for products etc. The customer will also have a relationship with the department store for the goods purchased.

Including additional service providers, for example, institutions who compile information like stock market information, or assist in conducting transactions will make these relationships more complex still, and should issues in m-commerce transactions arise, it will be essential to fully understand these to ensure that consumers are adequately protected.

11. Possible billing models

There are two billing models that have already emerged in Europe, and are likely to be adopted in the first instance in Australia.

11.1 Payment linked to mobile phone account

It is very likely that a number of models will develop for conducting sales transactions over wireless technologies. One current model is the telephone network operators, who already have the technologies developed for processing micropayments and billing very small amounts for transactions, will act as billing aggregators and take commission on the value of goods or services sold over networks in return for billing and collecting payment. The cost of the services or products purchased using the mobile phone technology will be billed to the mobile phone account.

Using the example of paying for parking using a mobile phone, a billing model that has emerged in Europe is a parking service that adds the cost of parking to a users phone bill. The system operates with a consumer calling a specified number and entering the number of the parking meter, and the time that parking will be required for, or sending an SMS to a specified number with the car's registration and code of the parking zone, and the charge is immediately added to the mobile phone account. In case the parking lasts longer than expected, the customer can add money to his or her account by calling a specified number. A call can

similarly end the parking time. The cost of the parking appears on the customers mobile phone account.

The standard billing model has meant that consumers with mobile phones receive their bills on a monthly basis for payment using a variety of mechanisms. In this sense, this model is similar to offering a consumer a line of credit. However, telecommunications operators also offer prepaid services, which would enable their customers to pre-pay the mobile account, which could be drawn on to pay for the parking and other services. Pre-paid cards also limit the risk for operators.

11.2 Linking payment to bank account

An alternative payment model could be the telecommunications operator retaining control over the organisation of payments, but with the bank being responsible for the billing and managing the finances as well as the transfer of funds from the bank account to the mobile account.

Using a second example of managing a parking payment, a consumer who wants to pay for parking using m-commerce would call a certain number to establish an account that would be managed by the telecommunications operator. In order to start using the account, the user would have to make an agreement with an Internet bank. The consumer would be able to load up the mobile account with funds that would be drawn on to pay for parking as well as any other services that had an agreement with the Internet bank managing the account of that consumer. In this case, the m-commerce arrangement performs more like a debit - or pre-paid account, rather than a credit account.

12. Issues associated with the introduction and uptake of m-commerce

The basic premise is that mobile consumers will want everything to work just as well as it does in the real world. They will want to be able to make m-commerce payments in the same way that they make e-commerce or physical world payments - easily, quickly, safely and with confidence.

This means that m-commerce transactions must share the same characteristics as all other payment card transactions - cardholder and merchant authentication, data integrity, privacy, confidentiality and non-repudiation.

It is essential that these issues be identified to determine the consumer protections that are currently in place, and those that need to be established to ensure that consumers are adequately protected before widespread uptake.

12.1 Privacy

Privacy issues have always been a key reason for potential online consumers to avoid eCommerce. In the early days of eCommerce, a significant fraction of consumers thought that credit cards could be "snatched" off the Internet. Solid encryption technologies has reduced most of those fears, and for the most part, new consumers don't worry about losing credit cards while online. However, there remain some very real privacy issues associated with conducting transactions electronically, which may be exacerbated with the capacity to undertake mobile transactions. These include unauthorized access to stored data, especially personal information and transaction history.

12.2 Security

Securing m-commerce may be even more difficult than protecting wired transaction. Constrained bandwidth and computing power, memory limitations, battery life and various network configurations all come into play, raise the questions as to whether there will be adequate security for users without compromising the ease of use and speed.

In the use of text messaging, a number of security issues have already been identified, and will extend to the use of m-commerce. While a direct SMS message is relatively safe because it is encrypted for its transition from one mobile handset to the other, because of its store forward nature, messages are vulnerable to being corrupted. Like voice messages, SMS' are stored on a server before being forwarded to the receiver. There is no mandatory encryption and access protection for storage. The only way to secure the entire transmission would be with end-to-end encryption.

Messages exchanged between two service providers can also be violated in transit if the link between the two networks is not protected. If this information is payment details or authorities to make transactions, there is even more danger.

The reliability of SMS messages is also in question. Unlike in Europe, where message delivery confirmation can be obtained by pressing a three-digit code, no confirmation is issued in Australia. The capacity to check and ensure that sent messages are received will be essential to build and maintain trust in the use of m-commerce.

Mobile technologies manufacturers are developing improved security for applications with authentication and encryption technologies. However, there are two tradeoffs for increased security, namely price and style.

12.3 Locational information

The nature of wireless networks and devices makes it possible to determine approximately where the user is located at any point in time, and, should they be travelling, the direction they are going. Mobile operators will be able to track calling patterns, and with eventual precision in positioning technology, will know where users are when they are conducting a transaction.

This makes it possible to deliver local information such as the locations of nearby stores, offices and emergency facilities backed up with connections to their wireless sites for information on services, hours and prices. Consumers can access local news or weather, or check on local housing prices. Essentially, the location of a wireless device can be used as one more search criterion in browsing the Web, focusing results on sites relevant to the user's immediate surroundings.

The adverse effects of this have meant that the Federal Trade Commission (FTC) in the United States has sought to ban the ability to determine a consumer's geographical location through the use of the wireless device. The concern of the FTC was raised because the technology allowed targeted, direct advertising and could also encroach on privacy rights if people were not given the option of deciding whether they want to be targeted in such a way.

12.4 Liability for transactions

The youth market for financial services has become increasingly competitive, and providers have started to tempt teenagers with offers of free advanced phones that can manage m-commerce applications, to sign up for specific accounts.

We have already seen the impact of this, with young people becoming drawn into expensive contracts that they cannot necessarily afford to maintain, with the promise of the smallest and most advanced mobile phone.

The ramifications of this could be exacerbated with m-commerce services, as young people become drawn into credit relationships, and purchasing services over their phone. How will the accounts of young people be monitored to ensure that they are not over committing in the use of these services, including how the content that consumers will be accessing is monitored and what sort of mechanisms will be put into place to restrict purchases that are legally prohibited, such as alcohol or pornography. Issues arise as to whether the Credit Code would provide adequate protection.

12.5 Relationships between service providers and consumers

There are a number of contractual issues that are likely to be raised with the introduction of m-commerce. For example, what responsibility will the network operator have for sales of inappropriate goods and services, for example, in the sales of cigarettes or R-rated movie tickets to minors if it participates in the billing and collection of such payments. Similarly, who will have the responsibility of checking information that the network operator collects and holds about customers, and their transactions.

The new relationships and third party alliances that m-commerce is likely to introduce will also raise concerns for consumers.

12.6 Disclosures and disclaimers

Using mobile Internet, there is a lack of protection afforded to consumers to inform them of their movements through the system. By way of example, in the traditional Internet, web-site operators have employed the use of a disclaimer to inform visitors to the site when they are actually leaving the site and moving to another site, or to exempt themselves from liability. Given the size of the screens, and the amount of information that will be able to be transmitted quickly, the effectiveness of a disclaimer can be questioned.

Firms will have to ensure that they deliver the correct information to customers within the required timeframes. This means that they will need to ensure that they can substantiate with the appropriate records, that their customers have seen the relevant warnings and disclaimers and have agreed to their terms and conditions. Given the size of the mobile phone screen, this may be difficult.

12.7 Advertising and selling practices

New selling practices are already emerging with the popularity of mobile phones, and this is likely to continue with mobile transactions.

In many ways, the written text that will characterise m-commerce could improve the capacity for consumers to prove advertising offers etc. However there are other issues likely to emerge, including the extent to which SMS messaging represents a form of unsolicited direct marketing. This is currently being considered, with the U.K. regulator Oftel increasing its powers to deal with unsolicited SMS messages.

12.8 Content

With regard to content transactions, the issue of who will be responsible for breach of regulations, i.e. the content regulator or the telecommunications regulator, will also require

consideration. It is anticipated that m-commerce, like the Internet, will be largely a *'pull'* rather than *'push'* medium, which questions who would be held liable for the transmission of illegal content.

There will be other issues that need to be considered, including the risk associated with legal liabilities such as defamation, obscenity, copyright, trade mark and patent infringement, data protection compliance etc.

12.9 Intellectual property issues

Broadband mobile delivery will enable data-intensive audio-visual information to be transmitted, and thus, there are likely to be considerable concerns with intellectual property issues, and transmission of content that is subject to copyright.

12.10 Standards and competition

In the longer term, competition problems may arise as a result of network effects. There is limited scope in the market for payment services for a large number of incompatible m-commerce payment processes. Users have a high preference for ubiquity. Firstly, a user wants the ability to send and receive money from other users. Secondly, a user wants to be able to use a payment function wherever he is. The usefulness of a payment system increases with the number of users, and a payment network is more valuable to each of its users the greater number of total users. This positive network externality favours the emergence of a standard and technical interoperability.

At the moment, as new systems are struggling to obtain precedence in the market, there is limited competition between m-commerce providers. There are many different schemes, each of which is trying to reach critical mass. At the same time, mobile payment systems will not stop at national borders. On an international level, multinational companies like large telecommunications companies, credit-card firms and technology providers will have a strong interest in setting a common standard.

A large number of interoperable schemes may restrict the adoption of m-commerce and hinder its future development. Thus, policy action might be called for in order to foster standardisation and the creation of interoperable systems. However, adopting standards at the early stage may result in sub-optimal standards being chosen, and hinder innovation. At the same time, coercive standard setting may not fully meet the needs of consumers in the market.

The existence of network effects calls for interoperability between the systems of different network operators. Interoperability can only be achieved by cooperation, which introduces a host of other problems, including the potential of collusive behaviour to the disadvantage of consumers.

12.11 Provision of credit

The extent to which m-commerce operators will be providing credit to enable purchases and transactions to be made is one issue that has the potential to raise considerable problems. Already, issues are emerging with young people finding themselves in mounting debt as a result of mobile phone subscriptions, and this, coupled with the capacity to pay for purchases that can be charged to your mobile phones could introduce significant payment issues. Credit providers will need to conform to the requirements under the Consumer Credit Act, which covers the provision of personal credit to consumers, however the extent to which this covers the access to credit for m-commerce applications could be ambiguous. It is often assumed

that the system will be regulated as a result of credit providers avoiding customers who pose a high risk, however this is questionable, particularly in the introduction of new services that are struggling to obtain market dominance, and could sign up customers that pose considerable credit risk.

12.12 Taxation

M-commerce is likely to present additional taxation problems. Some sites use Internet Protocol addresses to try to see whether a customer is in a particular tax jurisdiction, some try bank addresses, while others require social security numbers. Without an effective user ID program on mobile phones, it may be complex for government to determine payments that are being made via m-commerce.

12.13 Evidence and Enforcement

Perhaps one of the most important issues that regulators, including State and Territory and Federal regulators, will need to grapple with is how any existing and future consumer protection regulations, along with the other components in the broad regulatory framework will be able to be enforced with regard to m-commerce, and m-commerce providers.

A key question is evidence. How will consumers be able to prove that advertisers, marketers or companies have not adhered to the provisions in the various regulations or codes. Given the small size of mobile phones, the limited display options, and even the memory capability, it may be difficult for consumers to retain messages or content that has been sent to them on their phones for a period long enough to have the complaint recognised and dealt with. Furthermore, if the evidence is actually contained on the phone, in the form of misleading or intrusive content, how many consumers are likely to wish to give up their phones (and the number) for the purposes of providing evidence to any investigation.

12.14 Education and Awareness

Enforcement is also likely to be difficult given that mobile phones, and the messages that are sent or downloaded are usually only available to the individual who can see the screen and access the handset. An awareness and education campaign will be required to ensure that consumers are aware of their rights and obligations in the use of m-commerce.

13. Possible elements of a consumer protection framework for m-commerce

Despite the likening of m-commerce to other forms of electronic commerce, and the capacity to transact over the Internet, it is likely that there will be a dramatic difference between wireless and desktop Internet transactions.

We cannot assume that the rules will be the same for m-commerce as they are for e-commerce.

In order to ensure that consumers are protected in the use of m-commerce applications and services, there are a number of basic requirements that need to be fulfilled, including:

- Ability to authenticate the parties - each party must be able to authenticate the identity of the other party.
- Ability to authenticate the transaction - the consumer must be able to have confidence in the delivery of the genuine goods ordered and the merchant must be able to establish the genuineness of an order.

- Security of transaction - the transaction should take place in a secure environment; transfer of confidential information and goods delivery channels should be secure from external interference.
- Electronic evidence of transaction - a transaction log, including the offer of sale, order for goods, confirmation and payment authorisation etc, must be created and deposited in an unalterable format at a trusted repository from where it can be retrieved, in event of a dispute.
- Electronic contract - terms and conditions - each party must be able to establish an electronic contract easily and unambiguously with the details of the transaction, the terms and conditions of sale, and a contract sale.
- Payment protection - the payment must be guaranteed as well as protected.
- Ability to suspend, cancel or block transaction - consumers must have the right to suspend or cancel ongoing transactions like subscriptions to stock quotes. Similarly, they must also have the capacity to block unsolicited content from being delivered. Merchants must retain the right to suspend transactions if there is a breach.
- Ability to limit or reduce liability - consumers must have the capacity to reduce or limit the credit available, and similarly, merchants need the option to place consumers who are considered risks on limited credit.

14. Building a consumer protection framework

Already, a number of elements can be identified that will all come into play in supporting the development and uptake of m-commerce. These include:

- Education and information- consumers need to understand the risk to their personal well being in an unsecured transaction mechanism, and need to be motivated to care about and protect their personal information and transactions.
- Regulation - there is an important role for reasonable and appropriate government partnership and initiative through prudent legislative and regulatory guidelines
- Industry incentives - incentives need to exist to ensure that industry takes responsibility for protecting consumers, as a means of competitive advantage. Similarly, advertisers and marketers need to be motivated to not compromise consumers' personal information and not to gather and misuse information.

Ironically, many of the issues that are already emerging are already concerns in current use of mobile phones and the current provision of credit and general sales. For example, in the mobile phone industry, there are already a number of consumer issues such as the use of the lengthy contracts and difficulty in terminating a contract; problems of repairs; and liability if a phone is stolen. On the credit side, the problems of being charged for transactions that were not authorised; what happens when goods are delivered as faulty; and issues of liability are all current issues that need to be addressed in the context of m-commerce. Issues associated with excessive consumer debt cannot be ignored.

There is already a range of regulations in place that could have application to m-commerce, including the relevant national and state or territory specific legislation that m-commerce is likely to be regulated under. There are also likely to be a number of limitations in current legislation to protect consumers using m-commerce. For example, current fair trading legislation in Victoria requires adequate disclosure about terms and conditions of purchase. How will these be transmitted via a mobile phone given the limitations of the screen? Another example is in the provision of financial services advice online. Prior to doing this, a firm must obtain a considerable amount of information about a prospective customer. It is not

clear that these regulatory requirements can be met using a mobile phone as the small phone screens can show a maximum of 100 characters. It seems impractical and cumbersome to expect a customer to tap out the words on a mobile phone handset.

Nevertheless, there are options to improve consumer protection and consumer trust, including possible amendments to existing consumer protection frameworks, and industry-based approaches. For example, establishing trust marks might be one practical way to improve protection. A trust mark is a recognisable logo that can be granted to a business that is compliant with a code of conduct. However, as a recent study in the European Union has found, since trust marks have a recognisable brand value, there is now a proliferation of trustmarks on the web, leading to confusion and even raising certain doubts in the consumer's mind regarding their trust value. There is also significant disparity between various trust marks in terms of their scope and depth, which points toward the need for harmonisation and standards to promote confidence by consumers.⁵

15. Conclusion and invitation to comment

The purpose of this paper is to provide a very broad overview of what m-commerce is, and the sorts of issues that are likely to emerge that regulators must consider to ensure that consumers will be protected in using m-commerce services and applications.

At this stage, we are seeking comments from jurisdictions, including identification of consumer issues arising, any policy analysis currently underway, and whether or not there is support for coordinated work in this area.

For further information and to provide feedback, please contact Policy Officer, Tanya Swards, Consumer Affairs Victoria (CAV) on telephone (03) 9627 7179 or at tanya.sewards@justice.vic.gov.au

⁵ Cawdhry, P. & Wilikens, M. 2001, *Consumer Protection and Redress in e-Payments: Issues, Policies and Technologies*. IPSC Joint Research Centre, <http://www.jrc.es/pages/iptsreport/vol63/english/ICT5E636.htm> Accessed 22 April, 202.

REGULATORY FRAMEWORK FOR M-COMMERCE

The purpose of this section of the paper is to identify, and briefly discuss, the regulatory framework that will apply to m-commerce. This includes the different regulatory and self-regulatory bodies that will come into play in different m-commerce transactions.

The application of National Competition Policy on the development of m-commerce will be dealt with in the next stage of developing this paper.

1. Federal Regulatory Framework

1.1 Telecommunications Industry

The telecommunications industry is largely regulated by the Federal Government, with the State having some jurisdictional control over matters that relate to issues of fair trading. In 1997, with the passage of the *Telecommunications Act 1997*, the telecommunications industry was substantially deregulated and opened up to competition. As a result, the telecommunications industry became subject to general competition policy, while some industry-specific regulations have remained in place.

The development of mobile commerce will be subject to the legislative framework that has been established to deal with the provision and access to communications services, including mobile phones. This section provides a broad overview of the legislation, and the administrative structures that are in place to regulate the telecommunications industry.

Telecommunications Act 1997

The *Telecommunications Act 1997* provides the basis to open the telecommunications market in Australia up to full competition. With its introduction, the *Act* aimed to include a number of arrangements to protect and advance the interests of consumers, including the extension of universal service obligations, price controls for standard services, and the Customer Service Guarantee (CSG) which provides for standards for the connection of services, rectification of faults and keeping of appointments and for damages to be paid to customers where these standard are not met.

The CSG, which came into effect on 1 January 1998, provides for financial compensation by telephone companies to residential and small business customers where minimum performance levels in providing customer services, such as new connections and fault repairs, for standard telephone services are not met.

Under the *Act*, the regulation of the telecommunications industry has been brought more closely into line with general competition law as governed by the provisions of the Trade Practices Act 1974. As a result, the *Act* transfers a number of powers for regulation to the Australian Competition and Consumer Commission, and in keeping with the broad philosophy of competition policy, there is increased reliance on industry self-regulation, particularly in technical regulation and through the use of codes of practice to support the operation of the market and provide consumer safeguards.

1.2 Banking and Credit Industry

Like the telecommunications industry, the banking industry is largely subject to a federal regulatory regime. The year of 1997 marked a significant turning point in the structure of

Australian financial regulation. The Report of the Financial System Inquiry, known as the "Wallis Report", recommended changes to the regulatory structure.

The Wallis Report recommended that regulation be function-based, and that new regulatory bodies be given responsibility. The principle reason for this was the perception that the Reserve Bank of Australia ("RBA") was too closely associated with the banks. To counter this perception, the Australian Prudential Regulatory Authority ("APRA") was created and given the responsibility, previously exercised by the RBA, of prudential supervision.

Banking Act

The *Banking Act* covers the different types of organisations that are allowed to conduct banking activities and the way they conduct these activities. Under the *Act* an entity cannot call itself a bank without the consent of the Australian Prudential Regulation Authority (APRA). The following types of authorities are allowed to conduct banking business: a bank; a building society; a credit union and an authorised deposit-taking institution. As a result of the Wallis inquiry in 1997, a new class of financial institution was introduced into the legislation, the "authorised deposit-taking institution" (ADI).

The *Banking Act* is likely to apply to m-commerce transactions if these transactions can be defined as 'banking business'. An electronic payment system will amount to the conducting of banking business if it involves the "taking of money on deposit" and the "making advances of money" within the meaning of the *Banking Act's* definition of banking business.

The relevance of the ADI regulatory regime for electronic payment scheme participants is as follows. If the participant's activities in the scheme (or its activities generally) amount to "banking business", then they must apply for an authorisation or exemption from APRA. To fail to do so would expose the participant to civil penalties.

There is a growing body of statutory regulation, including the *Corporations Law*, the *Trade Practices Act 1974* (Cth) and the *Contracts Review Act 1980* (NSW), that extends to ADIs and affects their operations and administration.

1.3 Content and Information Provision

There are a range of regulations that have been devised to handle different types of content, including: content developed for broadcasting purposes, advertising and marketing content, and personal information.

The broad federal legislation that covers issues of content is the Broadcasting Services Act, which has application to material that is broadcast on the television or the radio, as well as information available on the Internet. It outlines a number of standards for content and information provision. The Federal government also regulates the handling of personal information, another form of content, through the privacy regulations.

Broadcasting Services Act

The legislative basis for the regulatory regime for Internet or other online content is the *Broadcasting Services Act 1992*.

In 1999, the *Broadcasting Services Act* was amended to incorporate provisions that could extend content regulation to encompass online content, including content on the Internet. The

Broadcasting Services Amendment (Online Services) Act 1999 addresses Internet content issues by:

- providing a mechanism for addressing complaints about Internet content;
- encouraging the development of codes of practice by the Internet industry; and
- educating and advising the community about ways to manage their, and their children's, use of the Internet.

The Federal Government took steps to introduce the co-regulatory scheme in response to legitimate community concerns about the nature of some online material and its easy accessibility. The scheme is based on the principle that what is illegal offline should also be illegal online.

The scheme applies to the activities of Internet service providers and Internet content hosts only. The Federal Government has stated that it will be encouraging the States and Territories to develop uniform legislation that will complement the Commonwealth legislation and cover the activities of users and content creators.

The *Broadcasting Services Act* will apply to the content that is transmitted over mobile phone technologies, in particular any information that is downloaded, including games and pictures, from the Internet, and advertising and marketing material that is sent to a consumer, or the consumer requests. New carriers that enter the market to offer m-commerce services will be required to comply with the content provisions in the *Act*, similar to those currently providing content on television or radio networks, or the Internet.

Privacy Act

The *Privacy Act* 1988 protects the way your personal information is handled by private sector organisations and government agencies. The Act covers the collection, use, disclosure, quality and security of personal information. It also gives you the right to access and correct your information.

In December 2001, the *Privacy Act* changed and now gives individuals new rights in relation to how personal information is handled by many private sector organisations. An individual's privacy rights are outlined in the ten National Privacy Principles (NPPs). These set the standards organisations are required to observe in collecting, storing, using, disclosing, protecting and transferring your personal information.

The new private sector provisions that have been incorporated into the *Privacy Act* apply to organisations (including not-for-profit organisations) with an annual turnover of more than \$3 million. The provisions also apply to all health service providers regardless of turnover. Businesses with an annual turnover of \$3 million or less are exempt from the new laws unless the business:

- is related to another business (for example it is a holding company or a subsidiary) that has an annual turnover of more than \$3 million;
- provides a health service and holds health records other than employee records;
- discloses personal information for a benefit, service or advantage;
- provides someone else with a benefit, service or advantage to collect personal information; or
- is a contracted service provider for a Commonwealth contract.

There are also exemptions for the media, and political parties and for information held in employee records. Some organisations have signed up to meet the standards of Privacy Codes rather than the NPPs. The Privacy Codes must provide protection at least equivalent to the NPPs.

The *Privacy Act* will have application on the ways in which personal information of consumers who use m-commerce services can be collected, as well as the ways in which their personal details can be used, in particular by advertisers and service providers. Telecommunications operators already handle large amounts of personal information about subscribers to mobile phone services, and with the introduction of m-commerce services, the amount of information collected on mobile subscribers by other parties, including banks and credit providers as well as traders, is likely to increase. All of these organisations will be bound to handle the personal information of individuals according to the principles in the *Privacy Act*.

Interactive Gambling Act

The *Interactive Gambling Act 2001* (IGA) is intended to limit access by Australians to some types of gambling sites on the Internet. The Act imposes obligations on ISPs, Interactive Gambling Service Providers, Publishers, Datacasters and Broadcasters for enabling providing access to prohibited gambling content. Companies who fail to comply with some obligations may be guilty of an offence against the Act.

Electronic Transactions Act 1999

The Commonwealth's *Electronic Transactions Act* commenced on 15 March 2000 and allows Australians to use the Internet to provide a range of Commonwealth departments and agencies with electronic documents which are as legally sound as traditional paperwork. It also allows people to communicate electronically with Government on a diverse range of issues, such as family law matters, research and developments grants and applications under Freedom of Information laws. The Act provides a light-handed legal framework to support and encourage business and consumer confidence in the use of electronic commerce.

This Act could be relevant where mobile phones are used as a communications means with Government. In June 2002 there was a suggestion that the Department of Workplace Relations, which managed Australia's unemployment contributions would use text messaging to contact people who had not submitted the correct forms to have their entitlements processed. This could evolve into a form of m-commerce, and, while it is untested at this stage, the *Act* could be broadened to encompass these forms of communication.

1.4 The regulators

The following regulators are involved in overseeing, and controlling the provision and access to telecommunications services in Australia.

Australian Communications Authority

The Australian Communications Authority (ACA), a Commonwealth Government regulator, is responsible for administering a range of technical and consumer issues relating to telecommunications, as well as managing the radiofrequency spectrum. The ACA licenses telecommunications carriers and reports to the Minister for Communications, Information Technology and the Arts on the performance of carriers and service providers. It is responsible for the allocation of licenses and spectrum, with technical standards and industry practices. The ACA has functions under the

Telecommunications Act, to issue carrier licenses and to regulate in regard to consumer and technical issues. It is also involved with monitoring and reporting on all significant matters relating to the performance of carriers and carriage service providers with particular reference to consumer satisfaction, consumer benefits and quality of service. Services covered in the ACA report include fixed and mobile telephone services; ancillary services (including operator assistance, billing, complaints and Directory assistance); emergency services; Internet services and pay TV services.

The ACA works closely with the Australian Communications Industry Forum, encouraging industry to develop voluntary codes of practice and technical standards where they are in the public interest and do not impose undue financial and administrative burdens on industry participants.

The ACA performs a key consumer protection function through administration of codes and standards, and in particular, the universal service obligation and customer service guarantee (CSG) provisions of the Act. The ACA has the capacity to enhance consumer protection arrangements should self-regulation fail, including the ability to set mandatory customer service standards. The ACA also administers the national numbering plan.

Australian Competition and Consumer Commission

The Australian Competition and Consumer Commission (ACCC) is an independent government body responsible for enforcement of the competition and consumer protection provisions of the Trade Practices Act 1974 and for prices surveillance, inquiries and monitoring. The ACCC was established by the Competition Policy Reform Act 1995 with the merger of the Trade Practices Commission and the Prices Surveillance Authority.

The ACCC has both general and specific powers in relation to the telecommunications industry. Under the Telecommunications Act 1997, the ACCC took over the regulation of competition in the telecommunications industry under two generalist provisions in the Trade Practices Act. These provisions are designed to facilitate the evolution of the telecommunications industry from the monopoly of Telstra (Telecom) to a fully competitive market.

The powers of the ACCC have been broadened and strengthened in a number of areas, including for example, to impose record-keeping rules on the telecommunications industry; to enable the ACCC to report and publicly release competition related data; to issue competition notices; and, in relation to enhancing the access arbitration process, the ACCC's roles in attending, mediating and arbitrating access negotiations.

Australian Securities Investment Commission

The role of the Australian Securities Investment Commission (ASIC) is to protect individuals and small companies in banking transactions. ASIC is responsible for ensuring that banks have in place various laws for dealing with customer complaints, and also reviews the banking practices of individual banks and sets guides for fee disclosure practices by banks. ASIC does not control bank fees and charges. ASIC are not responsible for credit.

With regard to banking practices, the role of ASIC is to protect consumers who make deposits in banks, credit unions and building societies by:

- setting standards about what they tell their customers
- monitoring their sales practices and compliance with codes of practice
- checking customer complaints systems and
- investigating and taking action against misconduct.

The Australian Prudential Regulation Authority (APRA) is responsible for the promoting the safety and soundness of deposit taking institutions and the Reserve Bank of Australia, is responsible for monetary policy and the stability of the financial system.

Consumers are also protected under State law administered by State Fair Trading Offices and against misleading and deceptive conduct by Commonwealth trade practices laws administered by the Australian Competition and Consumer Commission.

Australian Broadcasting Authority

The Australian Broadcasting Authority (ABA) was established by the Broadcasting Services Act 1992 (BSA). Among its other functions of planning for the provision of television and radio services, and monitoring compliance with the ownership and control provisions of the BSA, the ABA is charged with the regulation of material that is transmitted over broadcasting medium, including radio, television, Pay TV and the Internet. The ABA assists the different sectors of the television, radio and Internet industries to develop codes of practice relating to content and complaints handling and investigates complaints about inappropriate content on broadcasting services and the Internet. It also develops and administers program standards about Australian content and children's programs on commercial television and conducts research into community attitudes on programming matters.

The ABA is also charged with implementation of the recently passed *Interactive Gambling Act 2001*.

Federal Privacy Commissioner

The Federal Privacy Commissioner has responsibilities under the federal Privacy Act 1988 and is able to assist consumers who have complaints regarding privacy issues relating to Commonwealth or ACT government agencies, consumer credit reporting activities, tax file numbers and spent convictions. On 21 December 2001, the Commissioner will be empowered to investigate privacy complaints against private sector organisations as a result of the commencement of the Privacy Amendment (Private Sector) Act 2000.

2. State Regulatory Framework

The different elements of State regulation that could come into play in the regulation of m-commerce services and applications are outlined below. The extent to which each of these will apply to advertising, content provision and messages that are delivered via mobile phones, and other elements of m-commerce are yet to be explored, however, they are likely to have some application to the new services.

2.1 Telecommunications Industry

There is no telecommunications specific regulation that is administered at the State level. However, practices of telecommunications operators, including the contractual relationships that are established for the provision of telecommunications services, including mobile services and Internet service, and issues associated with sales of mobile phones and services. These broadly fall under the fair trading laws of each State and territory.

Fair Trading Act

In Victoria, the *Fair Trading Act* covers the conduct of industry and traders in the marketplace. This Act is very broad in its application, but includes provisions that include regulating traders in terms of:

- selling practices - allowing for cooling off periods in the case of contact sales (e.g. door to door selling);
- conduct of traders, including unfair and unconscionable conduct (when the power differences between the parties result in significant detriment to one party);
- product claims - the features that they attribute to a certain product, and other forms of misleading and deceptive conduct;
- disclosure of trading details - advertisers must include details of their businesses and address to enable those who wish to complain to direct their complaint to the appropriate person; and
- contractual practices - certain information must be provided on contracts between traders and consumers.

These provisions are likely to have an impact in the provision of m-commerce services, as well as the purchasing of goods and services using m-commerce applications.

2.2 Banking and Credit Industry

In addition to the provisions in the Fair Trading Act, the credit industry is also subject to specific legislation in Victoria that regulates the provision of credit.

Consumer Credit (Victoria) Act 1995

The Consumer Credit (Victoria) Act 1995 regulates the provision of credit in Victoria applies the Code in Victoria, which is known as the Consumer Credit (Victoria) Code. It was developed to give credit providers and consumers the same rights and obligations throughout Australia.

The Code was developed as a result of the State and Territory Governments *Australian Uniform Credit Laws Agreement*. Under the agreement, the Consumer Credit Code was first enacted in Queensland, known as the template legislation. The other States and Territories then passed their own legislation to adopt the Code. Any changes to the template legislation automatically apply in Victoria.

The Consumer Credit Code is intended to apply 'truth in lending' principles to all consumer credit transactions, including housing loans. Hire purchase agreements and some leasing arrangements are also covered.

2.3 Content and Information Provision

State Governments have not traditionally attempted to regulate content, however, some jurisdictions have established their own regimes to manage the collection, storage and use of personal information.

Information Privacy Act

A privacy regime was established in Victoria to cover the use of personal information by the State government. The *Information Privacy Act 2001* establishes a regime for the responsible handling of personal information in the Victorian public sector and is due to come into effect in September 2002. It identifies 10 principles that are compatible with the National Principles, to cover how information is collected and used by State government departments.

However, there has been little work on other forms of content regulation. Advertising and marketing practices have largely been left to industry efforts, and there are a number of industry codes that deal with content in advertising, as well as marketing and advertising practices.

2.4 The regulators

Office of Fair Trading

Each State and Territory has established an Office that oversees marketplace conduct, with a focus on protecting the rights of consumers in relationships with traders and industry. In Victoria, Consumer Affairs Victoria (CAV) administers over 40 pieces of legislation to regulate different segments of the marketplace, ranging from credit providers and real estate agencies to pawnbrokers and fundraisers. CAV is also responsible for the Fair Trading Act, and has wide-ranging powers to monitor and regulate the conduct of traders. The extent to which the *Fair Trading Act* will apply to m-commerce transactions and services has not yet been determined, however the Act is likely to have broad effect over issues such as the contracts for services and the claims that m-commerce operators make with regard to products.

There is also likely to be a role for CAV with regard to the credit issues that are likely to arise with the provision of m-commerce.

Privacy Commissioner

Victoria has established its own privacy commissioner, which is charged with overseeing implementation of the *Information Privacy Act*. Among its broad range of monitoring compliance and education activities, the Privacy Commissioner is also charged with responsibility to:

- assess and approve codes of practice submitted by public sector agencies and to review and recommend the amendment or revocation of approved codes of practice where necessary; and
- issue guidelines consistent with the *Freedom of Information Act* to assist agencies as they develop procedures for the handling of personal information, including its transfer outside Victoria, and develop their own privacy codes of practice.

The State privacy regime aims to encourage industry to establish their own regulatory framework to guide the handling of sensitive and personal information. These are likely to be industry specific, and could have application to m-commerce services for those industries that choose to develop a Code to manage the handling of personal information. Any Code that is developed must, at a minimum, afford the same protection to consumers as the *Information Privacy Act*.

3. Self Regulatory Framework

3.1 Telecommunications Industry

Australian Communications Industry Forum

The Australian Communications Industry Forum (ACIF) was established in May 1997 as the peak industry body to facilitate and manage telecommunications self-regulation. ACIF's main role is to develop and administer industry technical and operating arrangements that promote both the long-term interests of end-users and the efficiency and international competitiveness

of the Australian communications industry. Its primary functions include development of industry codes of practice for registration and the timely production of technical standards, specifications, plans and guidelines that the industry and community need.

Codes that have been developed by ACIF and registered that could have relevance in the provision of m-commerce services by telecommunications operators include:

- The Credit Management Industry Code: deals with suppliers' credit management and credit assessment of customers in relation to telecommunications activities, as defined in section 109 of the Telecommunications Act 1997, and is applicable to carriers, carriage service providers and content service providers.
- The Billing Industry Code: specifies the rules for the management of customer billing including bill content, billing verification and billing timeliness and the minimum standard requirements of a supplier's practices for billing.
- Call Charging and Billing Accuracy Code: specifies the requirements for checking the accuracy of call charging and billing of the standard telephone service in a multi-service deliverer, multi-network environment in Australia. It will assure end customers, regulators and government that carriers and carriage service providers provide an acceptable level of overall accuracy in the calculation of call charges. The code is intended to give customers confidence that call charging and billing is correct, and to ensure that carriers and carriage service providers are sensitive to consumer billing complaints.

Telecommunications Industry Ombudsman

The Telecommunications Industry Ombudsman (TIO) was established in 1993. The TIO scheme is a company limited by guarantee, operating at arms-length from industry and Government. Funding is derived from fees charged to members, based on complaints against members. The Act requires certain carriers and carriage service providers to enter and comply with the scheme.

The TIO provides a free, independent investigation service for residential and small business customers of telecommunications and services, including mobile and Internet services, who have been unable to resolve certain complaints directly with their telecommunications carrier, service provider or Internet service provider.

Service Provider Access Network (SPAN)

SPAN is the national industry association formed in 1993 to represent the service provider industry and organisations in related fields directly involved in the provision of telecommunications services to business and residential customers

Since its inception, SPAN has actively advanced service provider interests through participation in and contribution to the formulation of regulatory and legislative policy, industry codes and standards and carrier/service provider inter-working processes and practices. All SPAN members agree to be adhere to a Code of Ethics that outlines good business practices, ethics and professional behaviour.

3.2 Banking and Credit Industry

Banking Industry Ombudsman

The Banking Ombudsman Scheme was set up in 1990 to help individual bank customers sort out their unresolved complaints with their banks.

If the consumer has a dispute with a bank, he or she may take the complaint to the Banking Industry Ombudsman, the most elaborate of the dispute resolution mechanisms. The Australian Association of Permanent Building Societies has developed a model based on mediation and expert determination. There are four separate Credit Union Schemes:

Code of Banking Practice.

The Australian Bankers Association has developed the Code of Banking Practice to provide guidelines on how banks should deal with their customers. It requires the banks to provide personal customers with a free, external and independent process for resolving disputes. It is paid for by the banks as part of their service to you. More recently the Scheme was extended to allow small business to complain. However for small businesses which want more than an initial consideration of the merits of their case, a fee will be payable. This fee may be refunded depending on the outcome of the case.

Australasian Institute of Banking and Finance Code of Conduct

The Australasian Institute of Banking and Finance (AIBF) is a professional institute for individuals engaged in the banking and finance industry in Australia. The AIBF has its own Code of Conduct and its members are expected to be committed to a high standard of ethical conduct as outlined in the Code.

Electronic Funds Transfer Code of Practice

The Electronic Funds Transfer Code of Conduct is a voluntary code that applies to all transactions which are initiated by an individual through an electronic terminal by the combined use of an electronic funds transfer plastic card and a personal identification number (the PIN), or which are intended to be so initiated. It sets out rules about how electronic funds transfers should work and regulates various aspects of electronic payments, including the all-important problem of allocating losses in the event of a dispute. The Code sets out what the business must do, the rights and responsibilities of consumers and the avenues available, should a dispute arise.

The EFT Code does not cover business accounts or biller accounts. Biller accounts are accounts maintained solely to record amounts owed or paid for non-financial goods or services supplied by the company (eg an electricity account).

3.3 Content and Information Provision

Internet Industry Association

The Internet Industry Association has developed three industry codes of practice to regulate the provision of content over online networks, that could potentially be applicable to m-commerce content. These have been developed as part of the co-regulatory scheme that has been established by the ABA. The scheme aims to encourage use of the Internet and settle community concerns.

The scheme has three components:

- the establishment of a complaints online - hotline that provides a means for addressing community concerns about Internet content.
- the development of industry codes of practice by the Internet industry.
- the education of the community, monitoring content and other non-legislative activities.

The Australian Broadcasting Authority (ABA) registered three industry codes of practice on 16 December 1999 that outline the obligations of Internet Service Providers (ISPs) and Internet Content Hosts (ICHs) in relation to the range of Internet content matters set out in Schedule 5 of the Broadcasting Services Act 1992. The codes were developed by the Internet Industry Association (IIA) in consultation with industry, the ABA, and interested community groups and members of the public.

Content Codes 1 and 3 deal with a range of customer advice and content management issues. Under these Codes, ISPs will take reasonable steps to ensure that Internet access accounts ('access accounts') are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult. ISPs are also obliged to make those who create content that is hosted on the ISP site aware of their legal responsibilities with respect to the content that they develop and encourage them to use appropriate labelling systems, in respect of Content which is likely to be considered unsuitable for children.

Importantly, under these Codes ISPs are required to have procedures in place to deal with complaints from subscribers in respect of unsolicited email that promotes or advertises Internet sites or parts of Internet sites that portray information that could cause offence.

Specific provisions have also been developed for creating awareness about the way to make a complaint about Internet content, and for informing producers of Internet content of their legal responsibilities in relation to that content.

Content Code 2 specifies that if the ABA investigates a complaint about prohibited or potential prohibited content hosted outside Australia, it will notify the content to the makers filter software products listed in Schedule 1 to the code. For their part, ISPs are required to provide a 'scheduled filter' to each of their subscribers.

While these Codes are not mandatory, the *Broadcasting Services Act* provides that once the ABA directs an ISP or content host to comply with a registered code, they must then do so. This is similar to other codes currently operating in the telecommunications industry and forms the practical operation of co-regulation.

Early indications are that larger Internet service providers, who account for some 80 percent of end-users, are complying with their obligations under the codes but that a proportion of smaller ISPs may not be compliant with all measures particularly the provision of filters. The ABA and NetAlert are working with the industry on compliance issues.

Interactive Gambling Industry Code

The Interactive Gambling Industry Code has been developed by the Internet Industry Association (IIA) in response to the provisions in the *Interactive Gambling Act 2001*. The Act requires ISPs to assist, through the use of available technologies, to provide a means to prevent access by users to certain Internet content. It obliges ISPs to provide new customers with filtering software that has been approved for use in Australia. As part of this obligation,

ISPs must also provide them with adequate information to install and start using this software, or initiate the process as part of the registration of the customer.

The Code also places some obligations on the ABA, to notify companies developing the filtering technologies of the information that will identify gambling content which is prohibited, to ensure that the software is continually updated to identify, and filter this content.

Australian Communication Industry Forum Privacy Code

The ACIF Protection of personal information of customers of telecommunication providers expands the privacy protection afforded by the Telecommunications Act by setting rules for the handling of customer personal information. The Code is drawn from the National Privacy Principles to provide rules and guidance to telecommunications providers in the handling of their customers information.

The IIA is also currently developing its own Privacy Code that will be applicable to its members (including small business which is not subject to the national privacy regime) to provide guidance on the way that its members handle and use personal information of subscribers.

Short Message Service (SMS) Interoperator Issues - DRAFT Industry Code

The Australian Communications Industry Forum (ACIF) is current working towards developing a Code of Practice to handle the delivery of marketing messages to mobile telephone customers. It has been developed in response to the increasing amount of marketing and promotional messages, particularly unsolicited messages, that are likely to be sent via SMS text messaging technologies to an individual's mobile handset.

The Code covers the sending of marketing messages by carriers: the relationships between carriers and the commercial marketing bodies; and where exemptions can be available. Any commercial operator that is using a carrier to send marketing messages to its customers (subscribers to the mobile phone network) will be required to comply with the Code.

Once it has been finalised, it is intended that this Code will be registered with the Australian Communications Authority, under the *Telecommunications Act 1997*.

Advertising Codes of Ethics

Since 1998 advertising in Australia has been governed by a voluntary system of self regulation administered by the Advertising Standards Bureau. This system of self regulation is designed to complement other systems of regulation in the advertising environment, including the television and radio specific advertising codes of practice that have been established under the auspices of the Australian Broadcasting Authority (ABA) and the regulation through the various State and Commonwealth fair trading and consumer affairs agencies, who oversee issues of truth and accuracy in advertising.

Both peak bodies that represent advertisers in Australia, the Advertising Federation of Australia (AFA) and the Australian Association of National Advertisers (AANA) have developed their own Code of Ethics, however, the latter only applies to material that is published or broadcast, but not to material that is directly distributed to individuals (direct marketing) or Internet content.

While these self-regulatory systems are likely to have some bearing on advertising that is transmitted via mobile phones, given that these advertisements are being transmitted over the public spectrum, managed by both the ABA and the Australian Communications Authority. However, given that these Codes are focused on agencies that produce advertisements and do not cover direct sellers, the impact of these codes on the sort of advertising that is likely to be limited.

3.3.4 Australian Direct Marketing Association Code of Practice

In 1997 the Direct Marketing Model Code was released to provide guidance on what has been deemed to be 'appropriate' marketing practices, and prevent unreasonably intrusive practices by those industry groups who are involved in direct marketing.

The Model Code has been developed to encourage Industry associations who are involved in direct marketing, to establish their own codes of practice based on the provisions contained in the Model Code. Individual companies are also encouraged to adopt the standards set out in the Code.

In response to the development of the Code, the Australian Direct Marketing Association (ADMA) developed its own Code of Conduct, based on the provisions in the Model Code. Broadly, the ADMA Code identifies standards of fair conduct in relation to telemarketing, data protection and e-commerce standards including providing clear and unambiguous information about the identity of the businesses and the goods or services they offer, verifiable contracts, effective consumer complaint handling and security/authentication measures. A key feature of ADMA's Code of Practice is the establishment of an independent complaints body. The body investigates unresolved consumer complaints about members as well as non-member companies. Members will also be required to have their own internal customer complaints-handling procedures in place.

These self regulatory codes of practice and ethical principles are likely to come into play in the use of mobile technologies to advertise and send marketing messages, however, the only limitation is that these self regulatory frameworks are only applicable to the members of the relevant organisation.