Considering the implications of M-commerce – A Consumer Perspective

Issues Paper

Standing Committee of Officials of Consumer Affairs

E-commerce Working Party

Consumer Affairs Victoria

Victoria
The Place To Be

July 2004
eC-16-01-797

Making a submission

All interested individuals and organisations are encouraged to provide comments on this issues paper.

Comments in writing should be forwarded to:

The Convenor
E-commerce Working Party
Consumer Affairs Victoria
GPO Box 123A
MELBOURNE 3001

Email: mcommerce@justice.vic.gov.au

Closing dates for submissions is **30 September 2004.**

It should be noted that unless confidentiality for submissions is specifically requested, the contents of submissions may be made publicly available in any subsequent review process. Also, submissions may be subject to Freedom of Information and other laws and this should be taken into account when making submissions.

Further copies of this paper can be obtained by downloading it from the Ministerial Council on Consumer Affairs website **www.consumer.gov.au** or Consumer Affairs Victoria website at **www.consumer.vic.gov.au**

Executive summary

Introduction

Considerable advances have been made in the telecommunications and related industries to deliver content, applications and services to consumers using mobile telephones and other wireless devices.

M-commerce, which has been defined as *the use of a wireless terminal, such as a cellular telephone or personal digital assistant (PDA), and a network to access information and conduct transactions that result in the transfer of value in exchange for information, services or goods*, is likely to test the regulatory structures that are in place to deal with traditional transactions.

Services are already being rolled out that enable consumers to access content and services anytime, anywhere using their mobile phones. This could include using 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.

The Ministerial Council on Consumer Affairs (MCCA) recognises that these new services might raise issues of concern for consumers. As with the introduction of electronic commerce, and the use of the Internet, the uptake of mobile commerce, also known as 'm-commerce', is 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 may emerge which will test the adequacy of existing consumer protection mechanisms.

To provide a basis for a realistic examination of the consumer issues associated with m-commerce applications and services, the Ministerial Council on Consumer Affairs ("MCCA"), at its meeting of 2 August 2002, agreed to the establishment of a working party to further examine issues relating to mobile commerce.

The review is being conducted in two stages. In stage one, the working party is to report to MCCA on:

1. The anticipated availability and uptake of m-commerce services in the Australian marketplace in the short to medium term
2. The types of applications and services that are currently being developed for the Australian consumer market, and the emerging industry structure
3. The potential consumer issues that are likely to arise and industry approaches to providing consumers with adequate protection and support, and
4. International approaches to regulating m-commerce services.

Following this analysis, the working party was asked to make recommendations to MCCA on

1. Issues that need to be further considered to protect consumers and support the uptake of m-commerce in Australia, and
2. An appropriate role for governments.

This issues paper addresses stage one of the terms of reference.

The paper has been prepared through a combination of secondary research and a range of consultations with key stakeholders that will potentially have a role in the m-commerce industry, including telecommunications operators, financial service providers, content providers, security providers and some users. Based on analysis of these consultations, the paper identifies some key trends in the development of m-commerce, and likely future developments for the industry. The paper then identifies the existing regulatory safeguards that exist that will be applicable to m-commerce and the various approaches industry is taking to protect consumers and engender trust in m-commerce services.

Addressing the terms of reference for the study provides a basis upon which to consider whether additional consumer protection mechanisms will be required to protect consumers engaging in m-commerce.

The anticipated availability and uptake of m-commerce services in the Australian marketplace in the short to medium term

Looking at the trends in Australia's mobile telecommunications industry over the last 10 years, the improved capabilities of mobile technology and the increasing use of mobile services to deliver data (text) rather than voice communications, it is predicted that m-commerce will rapidly expand in Australia.

M-commerce is unlikely to replace other forms of consumer purchasing and, instead, is likely to be used as a convenient option for specific types of transactions. These could include low and high value transactions for both physical and non-physical goods. M-commerce is likely to become another choice for a consumer, rather than a preferred option, with the benefits and risks weighed up against other forms of buying and selling.

Key findings

- **M-commerce has some unique characteristics that differentiate it from other forms of e-commerce**
- **M-commerce services appear to be further advanced in Europe and Asia, predominantly as a result of a combination of high mobile phone and Internet penetration levels, the development of a larger range of services, and key regulatory and technical developments that aim to promote the development and uptake of m-commerce**
- **In the short to medium term (12 months to 3 years), m-commerce services are likely to be delivered using existing second-generation (2G) and enhanced 2G (2.5G) technologies and networks. This could result in the majority of transactions being reliant on SMS and text-based information between consumers and businesses**
- **Third-generation (3G) mobile networks, expected to be offered in Australia in 2003/04, are likely to drive the development of a wider variety of m-commerce applications, but the cost of these services may be an inhibiting factor**
- **The market for m-commerce services and transactions is expected to be driven by early adopters over the next 12 months, with the mass consumer market not contributing significantly to adoption until there is a variety of content and applications available, and the costs of services and the required technology decrease.**

The types of applications and services that are currently being developed for the Australian consumer market, and the emerging industry structure.

M-commerce will offer consumers another alternative to existing methods of purchasing goods and services. It will also offer merchants a new mechanism to deliver advertising and information products to consumers, as well as enabling instant transactions to be conducted.

Presently, the majority of m-commerce transactions that are being offered are for the purchase and payment of non-physical goods. This includes the purchasing of ringtones for phones and information services, such as cricket or rugby scores or stock-market updates that are delivered to the telephone handset. There have also been a number of trials that enable a consumer to pay for parking rather than using the traditional coin payment.

More complex m-commerce transactions are slowly emerging in the consumer marketplace. For example, recent trials conducted by Telstra Corporation and "Coca Cola" enable a consumer to purchase a drink from a vending machine and pay for it using a phone. This is likely to signal the emergence of an increasing trend towards the purchase of more goods using m-commerce.

At this stage most of the available transactions are relatively low in value, with the cost of the product and service being added to the customer's phone bill. However, as more diverse and secure payment mechanisms emerge, the capacity to conduct higher value transactions will also be offered to consumers.

International research and the consultations held with industry participants identified a number of trends.

Key findings

- **In the short to medium term, m-commerce services available to the consumer market are likely to be limited to those which represent relatively small values (micro transactions under $20). The purchase of telecommunications related products, e.g. ring-tones and games, is anticipated to continue to be popular, with limited niche services developing to enable transactions for non-telecommunications products**
- **Mobile phones are likely to continue to be the primary piece of equipment that are used to conduct m-commerce transactions in the short to medium term. In the longer term, new handsets and equipment are expected emerge to enable more complex transactions, including payment services**
- **It is anticipated that higher value m-commerce services supported by advanced billing or payment infrastructures will be available, however, these are not expected to be taken up by the mass consumer market in the short to medium term**
- **In the short to medium term, it is likely that key industries in the m-commerce value chain will develop partnerships to deliver m-commerce services rather than attempt to extend their reach into the provision of new services**
- **It is unlikely that any one player in the market is going to maintain dominance in the relationship with customers into the future. Co-operation between network operators, financial providers and content providers will be key to delivering m-commerce services.**
- **The lack of current standards for m-commerce and m-payments, and the proliferation of activities that are taking place in the race to create solutions may be hampering the development of m-commerce services**
- **A co-operative approach between agencies will enable a full consideration of the issues raised by m-commerce and the development of a regulatory approach that will stimulate the development of the m-commerce industry in Australia while providing suitable safeguards to users.**

The potential consumer issues that are likely to arise and industry approaches to providing consumers with adequate protection and support.

The review has found that m-commerce is likely to raise a number of issues and potential concerns for consumers. These extend far beyond the issues within the jurisdiction of MCCA and encompass issues such as privacy, security and content issues. Importantly, many of these issues will impact, not only on consumers, but also on merchants that are using m-commerce as another mechanism to broaden their reach to customers and support transactions.

The consultations conducted as part of this research found that a number of the potential issues that are likely to arise with the introduction of m-commerce are being addressed by industry operators, particularly in response to the increasing use of the Internet and the uptake of e-commerce. Industry-based responses such as codes of conduct to deal with the potential intrusiveness of direct marketing, practices to respond to the use of computers to conduct financial transactions, and protection mechanisms to deal with potential debt problems arising from the use of 1900 numbers have emerged in recent years. They will potentially apply to m-commerce to provide some additional protection to consumers, beyond those prescribed in regulation. However, m-commerce is also likely to enable consumers to undertake new and varied transactions which will not necessarily be covered by either existing legislation or industry-based approaches.

This paper identifies the key legislative protections that exist in Commonwealth, State and Territory law that will provide a basis for protecting consumers as they use m-commerce services. It also identifies a number of the specific industry-based approaches that have been developed to respond to consumer concerns that are likely to apply, or could potentially be extended to apply to m-commerce services.

The following issues have been identified for further discussion and consideration by regulators to determine whether current legislation, coupled with industry-based efforts, provide adequate protection for consumers

engaging in m-commerce. The discussion identifies issues beyond those that are the responsibility of fair trading agencies and which may need to be considered by other regulatory agencies as the popularity of m-commerce increases.

Fair trading

Risks posed by e-commerce, in particular those relating to distance purchasing, may be magnified when there is reduced ability to access information about the seller and/or the goods due to the limitations of the technology used, such as a mobile phone handset.

Key issues

- **How will m-commerce service providers ensure that consumers have access to required information (eg. terms and conditions of the transaction) and prove that consumers have agreed to such terms and conditions?**
- **Who will be responsible for providing information to a consumer about a product? Will there be some liability on the carriage service provider or will it be up to the supplier/service provider to provide this information?**
- **There exists a regulatory framework within Australia at both the Commonwealth and State and Territory level prohibiting misleading representations. Should legislation also provide for minimum information that should be disclosed to consumers at the time of making a purchase?**
- **Are current arrangements for the resolution of consumer complaints appropriate and adequate to deal with issues likely to arise from m-commerce?**
- **What options are available and suitable to hear and resolve consumer complaints in relation to m-commerce services?**

Financial

Financial issues are perhaps those that have been least rigorously tested in the context of identifying how the current regulatory frameworks will apply to m-commerce transactions. There are likely to be a number of consumer issues that will still require resolution, including security and liability issues. In addition, there may be a need to establish new processes to permit the use of mobile payments.

Key issues

- **Is the self-regulatory framework that has been developed adequate to deal with increasing electronic trade, both online and using m-commerce?**
- **What regulatory protections could be considered to improve consumer protection in electronic purchasing and payments?**

Privacy

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 unauthorised access to stored data, especially personal information and transaction history.

Key issues

- **What additional protections need to be put into place to protect consumers from receiving commercial advertising on their phones?**
- **How does Australian privacy legislation protect wireless information exchange?**
- **Will current privacy legislation protect consumers from their information being shared between service providers?**

Security

Securing m-commerce may be even more difficult than protecting wired transactions. Constrained bandwidth and computing power, memory limitations, battery life and various network configurations will all impact on the ability to provide adequate security for users without compromising the ease of use and speed.

Key issues

- **Should government have a role in implementing minimum security requirements for m-commerce transactions?**
- **What protections will be in place for a consumer if a mobile phone with commerce capabilities is lost? Who will liable?**
- **Should there be mandated levels of disclosure from companies involved in electronic transactions about the sorts of security systems used?**

Content

While the issue of ensuring appropriate content is not necessarily a fair trading issue, it does have some important implications in determining how the content market will develop. A more relevant issue for consumer protection and digital content is how consumers, in particular vulnerable consumers like children, will be protected from a plethora of content and the offer of goods and services that may not be suitable.

Key issues

- **How well will current content laws apply to the increasing use of mobile phones to access and transmit inappropriate content?**

International approaches to regulating m-commerce services.

Analysis of international responses to m-commerce show that there have only been a handful of specific regulatory responses to supporting the uptake of m-commerce or addressing specific consumer issues that arise with the introduction of m-commerce. These direct interventions focus on improving the transparency of m-commerce transactions for consumers and addressing key privacy issues associated with the potential intrusiveness of mobile technology when used for commercial purposes.

One interesting point that emerges is that these regulatory responses are targeted at telecommunications operators. This is perhaps because it is the telecommunications providers that, at this stage, are the primary provider of m-commerce services to consumers and are responsible for managing the customer relationship for the delivery of m-commerce services. However, as m-commerce services proliferate and become more complex, new operators become involved in the delivery, and the management of the customer relationship, and new payments systems develop to support costly transactions, it is likely that other forms of regulation will be considered.

The paper also identifies the existing international regulatory and self-regulatory regimes that could potentially apply to m-commerce services. There are a raft of laws in place that aim to protect consumers in relation to fair trading matters, financial services and e-commerce that will potentially apply to m-commerce transactions. Research undertaken as part of this review has not, however, identified any situations where these legislative approaches have been tested with regard to m-commerce.

Essentially, it appears that regulators around the world, while keeping a close watch on the way that m-commerce services evolve, are adopting a "wait and see" approach with regard to regulating these new services. There has certainly been no sustained effort to establish a series of new regulatory protections specifically in regard to m-commerce, and additional measures that have been put into place appear to focus on specific issues that have emerged in relation to these services rather than an over-arching regulatory response to m-commerce.

Conclusion

In conducting the review it has become clear that (a) m-commerce services are currently only at an early stage of development and there is still significant uncertainty as to the services m-commerce will support and the features of these services; and (b) many agencies will have a potential role in overseeing the introduction of m-commerce services.

Firstly, consultation with industry organisations has identified that there is still considerable uncertainty as to the way that m-commerce services will evolve. To a large extent, the capacity for m-commerce services to become an accepted alternative to other forms of shopping, including physical and electronic forms, will depend on the acceptability of the payment mechanisms that emerge, and the ability of operators to develop standard systems that will support interoperability. Other considerations, including the availability of content and services is another key factor in the development and uptake of m-commerce.

The review process has also identified that there are already a range of regulatory interventions that have been put into place that will potentially apply to m-commerce. Furthermore, as m-commerce services are developing, the industry is making some efforts to address key concerns for consumers. Any additional regulation needs to be considered in light of the current regulatory protections afforded by existing legislation and the various self-regulatory approaches that have been adopted by industry that will have application to m-commerce.

Secondly, agencies, including the Australian Communications Authority (ACA), consumer protection agencies including the Australian Competition and Consumer Commission (ACCC) and state and territory fair trading agencies, the Australian Privacy Commissioner and the Australian Broadcasting Authority (ABA) have begun to investigate their role in relation to supporting the development and uptake of m-commerce. The ACA has

recently released a discussion paper on the issues arising from m-commerce and the Commonwealth's E-Commerce Expert Group has identified m-commerce as an issue to be considered in terms of the Best Practice Model for E-commerce that is currently being reviewed.

Without adequate communication between regulators, there is the risk that the separation of powers, not only between regulatory agencies, but between jurisdictional and national levels could result in either duplication of effort or inconsistencies in approaches to m-commerce.

Next steps

The Working Party recommends that developments in m-commerce, including technological and market developments, as well as regulatory developments, both nationally and internationally, be closely monitored over the next 12 months. This will provide consumer protection agencies with a stronger basis upon which to determine the key issues that need to be addressed by government to protect consumers. It will also give regulators an opportunity to hold further discussions and explore the potential roles that different agencies could play to support the introduction and uptake of m-commerce in the Australian consumer market.

A co-operative approach between agencies will enable a full consideration of the issues raised by m-commerce and the development of a regulatory approach that will not hinder the development of the m-commerce industry in Australia.

Recommendations of the Working Party

1. That MCCA agree to the public release of this report.
2. That the SCOCA E-commerce Working Party continue to monitor market and regulatory developments relating to m-commerce over 12 to 18 months from release of this issues paper.
3. That regulatory agencies continue to liaise regarding the issues being raised by m-commerce and consider the development of a regulatory approach that will provide suitable safeguards to users.
4. That a further report on m-commerce developments and issues be prepared for MCCA in 2006.

Contents

List of Tables

List of Figures

"Section 1 Introduction and Overview"

1

Considerable advances have been made in the telecommunications and related industries to deliver content, applications and services to consumers using mobile telephones and other wireless devices.

Services are already being rolled out that enable consumers to access content and services anytime, anywhere using their mobile phones. This could include using 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.

The Ministerial Council on Consumer Affairs recognises that these new services, while offering a new way of conducting transactions, and bringing many benefits to consumers, could also raise some concerns. As with the introduction of electronic commerce, and the use of the Internet, the uptake of mobile commerce, also known as 'm-commerce' is 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 may emerge which will test the adequacy of existing consumer protection mechanisms.

The purpose of this review, therefore, has been to develop a more realistic assessment of the sorts of m-commerce services that are likely to be available in Australia over the next two to five years and to identify the implications these services may have for consumers.

The study is intended to provide a basis upon which to consider whether additional consumer protection mechanisms will be required to protect consumers engaging in m-commerce.

For the purposes of this paper, m-commerce has been defined as *the use of a wireless terminal, such as a cellular telephone or personal digital assistant (PDA), and a network to access information and conduct transactions that result in the transfer of value in exchange for information, services or goods*[1].

1.1 E-commerce Working Party

The Ministerial Council on Consumer Affairs ("MCCA"), at its meeting of 2 August 2002, agreed to the establishment of a working party to examine consumer issues associated with m-commerce applications and services.

The E-commerce Working Party was established to consider a number of issues relating to protecting consumers who are conducting commercial transactions using new technologies, including the Internet and mobile phones.

[1] The definition of 'm-commerce' is not set in stone. Some organisations adopt a narrow definition that limits m-commerce's scope to mobile payments, or to the mobile telephone network. Some broaden its scope to include all B2B and B2C wireless interactions, or to wireless links to any network such as the Internet.

Other projects currently under consideration by the Working Party are:

- the need for a set of basic, uniform statutory measures to protect consumers engaging in online transactions
- the need for a common extra-territorial regime for State/Territory Fair Trading legislation
- web seals of approval.

The E-commerce Working Party comprises representatives from the following agencies:

Consumer Affairs Victoria (Project Convenor)

Department of Consumer and Employment Protection, Western Australia

Competition and Consumer Policy Division, Department of the Treasury, Commonwealth

Office of Fair Trading, NSW

Office of Consumer Affairs & Fair Trading, Tasmania

Office of Consumer and Business Affairs, South Australia

Australian Competition and Consumer Commission

Department of Tourism, Fair Trading and Wine Industry Development, Queensland

Department of Justice & Community Safety, ACT

Consumer and Business Affairs, Department of Justice, Northern Territory

Ministry of Consumer Affairs, New Zealand

1.2 Addressing the Terms of Reference

The Working Party has been asked to report to MCCA in two stages. The first stage explores recent and anticipated market developments in order to identify the sorts of m-commerce services that will be available in the short to medium term (12 months to 3 years) in Australia. The second stage involves a more rigorous assessment of the implications these services may have for consumers, the approaches industry is taking to protect consumers and engender trust in m-commerce services and whether additional consumer protection mechanisms will be required to protect consumers engaging in m-commerce.

Stage One

To report to MCCA on:

1. The anticipated availability and uptake of m-commerce services in the Australian marketplace in the short to medium term
2. The types of applications and services that are currently being developed for the Australian consumer market, and the emerging industry structure
3. The potential consumer issues that are likely to arise and industry approaches to providing consumers with adequate protection and support, and
4. International approaches to regulating m-commerce services.

Stage Two

To make recommendations to MCCA on:

1. Issues that need to be further considered to protect consumers and support the uptake of m-commerce in Australia, and
2. An appropriate role for governments.

1.3 Where we are up to

This paper addresses the key terms of reference for Stage One of the m-commerce project. It provides an analysis of the current and anticipated developments in the provision of m-commerce services in Australia.

A better understanding of the range of services that are likely to be available for purchase, from ring-tones to movie tickets, will provide a basis for a more detailed appraisal of the issues that will probably emerge for consumers and regulators. These include how can an m-payment be proven, how can consumers seek redress in situations where goods are faulty or not delivered and what support will be available to consumers who have financially over-committed to an m-commerce service. Other issues that will not necessarily fall under the responsibility of consumer protection agencies, such as privacy and security, are also considered as part of this issues paper.

The paper is not a proposal for regulatory action, but rather aims to identify situations where potential issues may arise and explore whether there is a role for government in addressing these issues, taking into account current regulatory consumer protection safeguards and industry approaches.

1.4 Methodology

The paper has been developed based on a series of discussions with key stakeholders who are or are likely to be involved in the development and delivery of m-commerce services and applications. Over 30 industry organisations were contacted representing all sections of the m-commerce value chain, including applications and service developers, content providers, telecommunications carriers and service providers, handset manufacturers, and payment systems providers, including bank and credit providers. This process resulted in a series of in-depth discussions with a number of organisations. A number of written submissions were also provided.

To provide a basis for discussions, Consumer Affairs Victoria (CAV) prepared a preliminary paper that raised a range of key issues and questions for consideration in the submissions. Key points from the earlier paper have been integrated into the development of this issues paper. This preliminary discussion paper is available on the CAV Website at www.consumer.vic.gov.au.

The project has also involved research using international and national journals, newspaper reports and reports found on websites. Ongoing searches have also been undertaken on websites of companies reporting on or producing m-commerce services and applications. This secondary research has provided a valuable source of information on international developments, the roll-out of m-commerce services and the sorts of issues industry is grappling with in stimulating development and uptake of m-commerce services.

The project is being coordinated by Consumer Affairs Victoria on behalf of the SCOCA E-commerce Working Party.

1.5 Scope of the paper

The purpose of this issues paper is to address the terms of reference.

The issues paper provides a descriptive analysis of the developments in the m-commerce market internationally and in Australia. The focus is on products and services that are being rolled out to the mass consumer market, rather than applications designed for the business market.

The experience with most new forms of technology is that services are typically developed for high-end users, who are willing to pay and have the greatest use for new services, then trickle down into the consumer market as they become more affordable and more readily available.

While m-commerce applications that are currently being developed for business and government could eventually become available to consumers and provide pointers to the sorts of issues that are likely to arise, this issues paper examines services that are targeted to consumer markets. The focus is on services that support general consumer behaviour – shopping, seeking information, making purchases and conducting transactions.

1.6 Limitations of the issues paper

This paper does not cover all the issues that m-commerce is likely to raise, including the broader range of copyright and content issues, security and data quality issues and broader problems of fraud and theft.

Given the breadth of the issues that m-commerce is likely to raise, it is impossible to document all of these and cover the various international experiences with each of these. Furthermore, the experiences and the issues that arise in each jurisdiction are likely to differ, meaning a comprehensive coverage of all issues is impossible.

The paper attempts to identify a number of the key consumer issues that are likely to emerge as m-commerce services gain popularity.

1.7 Structure of the issues paper

Section Two of the paper addresses the first two terms of reference for the study. Based on the primary research conducted with key stakeholders, the paper identifies the anticipated availability and uptake of m-commerce services in the Australian marketplace and considers the types of applications and services that are being developed for the consumer market. This section also identifies the emerging industry structure, key players in the delivery of m-commerce and likely future developments for the industry. For each of these, some conclusions are drawn regarding the potential future of m-commerce in Australia and the sorts of issues that are likely to impact its further development.

Section Three of the paper is focussed on identifying the potential consumer issues that are likely to arise and industry approaches to providing consumers with adequate protection and support.

The analysis identifies five key categories:

- fair trading;
- financial;
- privacy;
- security; and
- content.

For each of these sub-sections, the paper identifies possible issues that are likely to arise for consumers; the current Australian laws that could potentially have some application to responding to the issue; and industry-based responses that have emerged to deal with potential issues, and the capacity of these to extend to m-commerce transactions. Where there are international laws or approaches that go further to provide additional protection to consumers, and where these could potentially apply to m-commerce, these examples have been identified and explored. It is beyond the scope of this paper to review all international regulation that will potentially apply in these areas, so key approaches have been identified. The purpose of this approach is to provide some examples of possible regulation that could be considered in Australia to deal with new forms of commerce and the potential consumer issues these raise. It is beyond the scope of this issues paper to consider other potential roles of government in stimulating demand for m-commerce.

Based on this analysis, the paper goes on to identify a number of key issues for further consideration by regulators, industry and consumer bodies. The issues considered in Section Three extend beyond those that are the responsibility of fair trading and consumer protection agencies. However, the purpose of this broader discussion is to identify the range of potential issues that m-commerce raises for consumers, and to bring these matters to the attention of other regulators and relevant bodies for consideration.

The intention of this section is to provide a framework to consider whether the current mechanisms in place provide a regulatory environment which can promote the development of the m-commerce market, and ensure that adequate safeguards exist to support uptake of m-commerce by consumers.

It is not the purpose of this document to make recommendations on a role for governments in protecting consumers who use m-commerce services.

Section 2 Scoping the M-commerce market

2

2.1 Australia's mobile telecommunications industry

Australia's mobile telecommunications industry has performed strongly over the last 10 years, making a substantial contribution to the wider telecommunications industry and the Australian economy.

There are an estimated 14 million mobile phones in use by 65 per cent of the Australian population in over 50 per cent of households. Australia's mobile penetration rate ranks Australia fourth in terms of market development in the Asia-Pacific region. Internationally, it is estimated that there are 1.3 billion mobile users.[2] While growth has slowed in the last few years, even the lowest growth rate in 2001 was associated with a 10.6 per cent increase in subscriber numbers. The growth rate in mobile subscriber numbers between 2002 and 2003 was 13.5 per cent.[3]

As mobile telecommunications technology continues to develop, there is increased use of data compared to voice services. In 1998, data revenue accounted for only one per cent of total carrier revenue. By 2002, this had increased to 7.5 per cent and the trend is expected to continue. The following table shows the Average Revenue Per User (ARPU) of data and voice components.[4] Expectations for future industry growth point to increased data usage.

Table 1: Average Revenue Per User

	2000	2001	20002
Data services	0.67	2.30	4.20
Voice services	66.79	58.31	51.70
Total ARPU	**67.46**	**60.61**	**55.90**

The economic significance of the mobile telecommunications industry must be considered in broad terms, which include industry revenue, contribution to industry development, innovation, employment, capital expenditure by the industry and contribution to taxation and government revenue (such as through purchasing of spectrum, payment of taxation etc).

Mobile telecommunications also has an impact on some social measures. For many people, mobile telecommunications is more than a tool to make voice calls. The extensive array of services and information available means that the mobile phone can make 'life more mobile'. A significant benefit of the mobile phone continues to be the ability to reach people on the move. This has become important for business and has driven the development of a range of innovations that are built on voice and data communications via mobile telephony.[5]

[2] Allen Consulting Group, 2003, Australian Mobile Telecommunications Industry: Economic Significance, September 2003, Research Commissioned by the Australian Mobile Telecommunications Association, AMTA

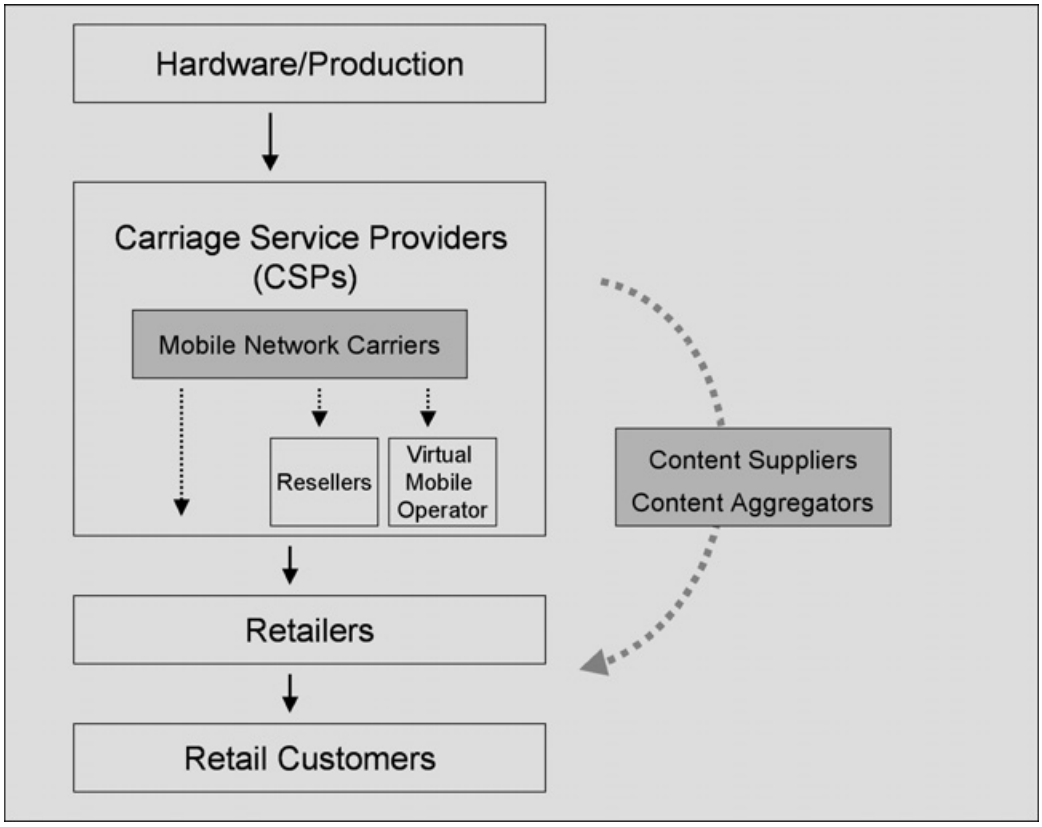
[3] ibid. p.16

[4] ibid. p.23

[5] ibid. p.xi

The current industry structure involves a number of sectors that in combination provide the services that make mobile telecommunications available to final customers. This is outlined in the following diagram.[6]

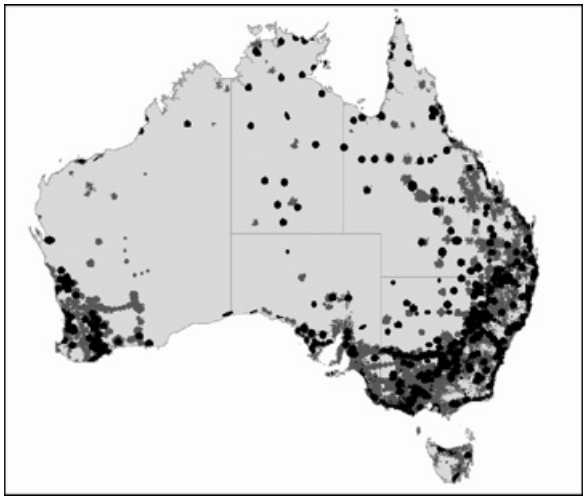
Figure 1: Delivering mobile services to a consumer



Australia's mobile phone services are reaching close to 98 per cent of Australia's population, across just 20 per cent of the landmass. The coverage provided by individual mobile operators varies from place to place, however the use of 'roaming agreements' means that many customers will still have access to mobile service networks even if their provider hasn't covered a specific area. The following figure shows the coverage of mobile services across Australia.[7]

Figure 2: Mobile telecommunications coverage in Australia 2002

One hundred per cent mobile coverage of Australia is provided through satellite mobile phone systems.



[6] *ibid*. p.5

[7] Department of Communications, Information Technology and the Arts (DCITA), 2002, A Users' Guide to Australian Telecommunications, 12 November 2002 http://www.dcita.gov.au/ Accessed 24 October 2003.

2.2 Defining m-commerce

There is considerable divergence in the definitions of what sorts of services m-commerce includes. Some organisations adopt a narrow definition that limits m-commerce's scope to mobile payments or to the mobile telephone network. Some broaden its scope to include all business-to-business (B2B) and business-to-consumer (B2C) wireless interactions, or to wireless links to any network such as the Internet.

For the purposes of this paper, a starting definition for m-commerce is …

> *the use of a wireless terminal, such as a mobile telephone or personal digital assistant (PDA), to facilitate the exchange of goods and/or services, including information.*

This paper focuses on the delivery of content, applications and services to consumers, or B2C m-commerce. Such services may enable consumers to use wireless devices to access bank accounts, receive news or promotions and buy products.

It is noted that in some submissions to the Australian Communications Authority (ACA) examination into m-commerce, there was a perception that the definition of m-commerce should exclude traditional financial transactions such as bill payment and the use of a credit card to make a purchase via a mobile phone voice call. Thus, limiting the concept of m-commerce to a data transaction.[8]

2.2.1 Convergence across technologies and services

M-commerce is an example of the convergence of technologies and services to deliver new capabilities to consumers. M-commerce enables the delivery of different services, that were traditionally delivered across separate networks, to be delivered across a single network.

Network convergence is the integration of voice, data, video transmissions and multimedia applications on the same transport media. It enables a single network to deliver voice communications, data services, financial services and other forms of content – including broadcasting messages and the Internet.

However, the extent to which this convergence will extend beyond network convergence to the convergence of service providers is less certain. As will be discussed in this paper, it appears that while the technologies will converge, service providers will continue to specialise in the delivery of their specific areas of expertise, at least in the short-to-medium term. Hence, telecommunications providers will not automatically begin to deliver financial services and banks will not become telecommunications providers. Instead, it is likely that partnerships will develop to enable the potential offered by network convergence to be fully exploited by service providers who retain their specialist roles.

2.2.2 Is m-commerce the same as e-commerce?

The extent to which m-commerce is a derivative of e-commerce has been questioned, particularly in the context of the regulatory structure.

In considering its evolution, m-commerce is the extension of e-commerce beyond the limitations of the PC or TV as access devices. To engage in e-commerce, a consumer must purchase hardware (a computer), then pay an Internet service provider (ISP) for an Internet connection, and then go to a website to purchase an item.

M-commerce is the same. A consumer must buy hardware (a mobile telephone or PDA), then pay a wireless service provider for a data connection, and then purchase an item from within a wireless portal (or 'walled garden') or from an Internet site.

There are a number key differences between e-commerce and m-commerce that must be considered in examining how such services should be treated in the market. As noted by the ACA, the following points of difference exist:[9]

- mobile users are more likely to use a voice channel than an e-commerce user
- location awareness/dependence is specifically an m-commerce capability
- m-commerce users are more likely to be moving from jurisdiction to jurisdiction, and
- m-commerce devices tend to have more limited text handling capabilities.

[8] ACA, 2003, *Mobile Commerce Regulatory and Policy Outlook Discussion Paper: Summary of submissions*. October 2003, http://www.aca.gov.au

[9] *ibid*.

There are two key features of mobile phones that differentiate them from other technologies:

- a device, the SIM card, that can store key information about an individual that links an individual to a phone, and
- the use of radio-frequencies to transmit information means that the location of the phone can be identified and tracked.

These factors must be examined in considering whether additional regulation is required to support m-commerce transactions and protect consumers using m-commerce services.

Finding 1: M-commerce has some unique characteristics that differentiate it from other forms of e-commerce.

2.2.3 Does m-commerce require an Internet connection?

A further distinction must be made between m-commerce and mobile Internet. The assumption is often made that to conduct m-commerce there is a need to have access to the Internet. Perhaps a contributing factor to this perception has been the introduction of I-mode offered by NTT DoCoMo in Japan, which has enabled millions of people to use Internet-enabled phones to send emails, check horoscopes and access email content. While m-commerce transactions can occur using the Internet, there are also more direct transactions that can occur without accessing the Internet.

The Internet includes web sites operated by both common carriers and sites operated by unrelated third parties. Whether accessed through traditional phone lines, new broadband services or through wireless services, the Internet is largely an open network where transactions can occur with any supplier.

Finding 2: M-commerce services are likely to encompass transactions directly between a consumer and a business entity that do not necessarily require access to the Internet.

Mobile Internet could provide one platform across which to conduct m-commerce transactions and is likely to become more widely available in Australia over the next five years, particularly with the rollout of 3G services.

2.3 International market developments

Much of the early availability and take-up of m-commerce services has been within Europe and Asia and has occurred during the past 18 months. The dollar value of global m-commerce activity is forecast to reach US$37 billion by 2007[10], up from US$6.7 billion in 2002. International reports have provided some overwhelming estimates of the predicted size and worth of the m-commerce market.

2.3.1 Europe

In Europe, where penetration levels for mobile phones have reached 30 per cent, it is estimated that 10 per cent of the adult population will be mobile Internet users.

KPMG predicts that the market for m-commerce in Europe alone is estimated to be worth 23 billion euros. One of the key drivers of this growth is the significant uptake of wireless devices, including mobile phones and more advanced technologies such as PDAs. These are continuing to be developed with wireless computers linked with a mobile phone emerging in the consumer market.[11]

Revenues to mobile telephone companies and content providers from telephone handset screen logos and ring tones alone generated US$2.9 billion in Western Europe in 2002[12]. 3G services in several European markets are beginning to sign up customers.

2.3.2 United Kingdom

There is little awareness of more advanced m-commerce services to date in the United Kingdom. In 2002, 60 per cent of Internet users said they had no intention of ever using a mobile phone to access the Internet and most find the idea of emailing, banking, or searching for information on a mobile wholly unappealing[13]. This is likely to change as the technology develops.

[10] Ovum, 2002, M-Payment: The second stage of m-commerce, Ovum research paper

[11] Cahners In Stat 2002

[12] NOP World and Mobile Metrix study quoted at http://www.mcommercetimes.com/Technology/317

[13] Which? *Online Annual Internet Survey 2002*, http://www.which.net/surveys/

At May 2003, only 2 per cent of UK mobile users are able to use MMS (Multimedia Messaging Service). However, people aged 15-34 spent US$95 million on ring tones, US$78 million on logos and US$142 million on SMS (Short Message Service) alerts in 2002[14].

2.3.3 Japan

Japan's I-mode service, released by NTT DoCoMo in February 1999, is one example of a success story for mobile Internet services. At February 2003, close to 80 per cent of Japanese mobile telephone owners were subscribed to wireless Internet services, such as NTT DoCoMo's I-mode[15]. With 1 million new subscribers joining each month, I-mode is now the largest Internet access platform in Japan.

I-mode subscribers have access to a number of m-commerce services. In addition to buying tickets, ordering books and getting the news delivered to a mobile handset, subscribers can carry out banking transactions with up to 280 banks and securities brokers.

Several Japanese carriers have already launched 3G services.

2.3.4 Singapore

The value of m-commerce in Singapore has been predicted to reach US$403 million by 2005[16]. Young people in the Asia-Pacific region currently spend almost 14 per cent of their total leisure spending on mobile products[17]. Singapore Telecommunications (SingTel) launched a corporate text messaging platform for promoters and advertisers in 2002. BizLive SMS had signed up 100 customers to its permission-based SMS marketing service at June 2003[18].

2.3.5 United States

The US is lagging behind Europe due to an earlier lack of a standard for mobile phone network technology. SMS is only now becoming popular as carriers roll out new networks.[19] However, the market is expected to develop rapidly once m-commerce takes off in Europe.

It is expected that the number of Internet-enabled mobile devices will exceed the number of PCs by the end of 2003.[20] Another research centre, the Yankee Group, similarly predicts that by 2004, more than 30 per cent of all wireless users will access the Internet through mobile devices.

Finding 3: M-commerce services appear to be further advanced in Europe and Asia, predominantly as a result of a combination of high mobile phone and Internet penetration levels, the development of a larger range of services, and technical developments that aim to promote the development and uptake of m-commerce.

2.4 Market development in Australia

Australia and New Zealand are following Europe's lead and are likely to see similar levels of uptake given the nations' histories as technology adopters. Growth in the mobile market has been outlined above, and other developments are occurring simultaneously.

Industry initiatives in m-commerce

In Victoria, the "mCommerce Centre" has recently been launched at Monash University. The Centre is conducting applied research into mobile technology and aims to use the results to assist Victorian businesses and stimulate adoption of mobile technology. One of the key features of the Centre is that it aims to draw together representatives from industry and business and researchers from other disciplines to promote collaboration and examine the relationship between information technology, mobility and business processes.[21]

2.4.1 Lessons from SMS

In Australia, the use of mobile telephones for sending text messages has increased dramatically in recent years, which

[14] NOP World and Mobile Metrix, *op cit*.

[15] IDG news article 19 Feb 2003

[16] IDC, Asia-Pacific M-Commerce Forecast and Analysis - Opportunities Await, October 2002

[17] Mobile Youth 2003 report, W2F

[18] *Singtel sees strong demand for corporate SMS communications services*, SingTel press release June 2003

[19] In 2003, only 10-15 per cent of phones can receive text messages and other data, Ralph Simon, director of Mobile Entertainment Forum, quoted in The Age, 9 June 2003

[20] Gartner Group, 2002, *'U.S. M-Commerce Market: Slow to Develop'*, M-14-5621 31 October, 2002

[21] Monash University, Monash Magazine, Autumn/Winter 2003, Issue 11

points to a significant potential market for m-commerce users. Paul Budde's (2002) estimate that 300 million text messages are sent by 11.5 million mobile telephones over the three Australian mobile networks each month, demonstrates the appeal of non-voice forms of communication.

SMS is available on the three Australian GSM mobile networks. Telstra, SingTel Optus, and Vodafone have signed agreements allowing messages to travel from one network to another. This has boosted SMS usage to the point where a very high proportion[22] of mobile phone users are familiar with it, making it a popular, emerging delivery channel for marketers[23].

SMS provides a channel for the delivery of information alerts and content. SMS is available on almost all GSM networks worldwide, and has paved the way for Enhanced Message Service (EMS) or Multimedia Messaging Services (MMS). Based on SMS technology, these new technologies give consumers the ability to send superior quality graphics and photographs. It is expected that the number of people worldwide with MMS-capable handsets that can receive picture or video messages will jump significantly in the medium-term[24].

Currently the main users of SMS messages in Australia are people under 25, who send an average of five messages a day.[25]

2.5 Who will be using m-commerce

While strong trends have yet to emerge, it is expected that m-commerce growth will be driven by young adults and business people.

The experience in other countries with the uptake of Internet-enabled phones shows that growth is likely to come mainly from younger, under 18 year olds and mature, 55+ consumers.[26] However, the trends are likely to differ for m-commerce, particularly as transactions become more complex and payments are made possible. While the youth market (13-18 years) has been the largest user of text messaging to date, it is unlikely to become the target market for m-commerce due to legal restrictions in contracting with minors and the lack of a significant income. Given the young adult acceptance of online and mobile use, it is predicted that the greatest segment of m-commerce early adopters will be young adults, aged between 20-35 years. M-commerce is also predicted to be attractive to professionals in the 30-45 age bracket who use their mobile phone daily and are likely to adopt work-based transactions.

2.6 Factors influencing development

The availability and take-up of consumer m-commerce depend on a number of factors, including:

- network infrastructure
- cost of services
- availability of applications
- hardware and handsets
- consumer sentiment
- integrity and security of transactions
- payment and billing systems
- operator models
- interoperability and standards, and
- regulatory framework.

2.6.1 Network Infrastructure

Currently, most of the m-commerce services that are being rolled out use existing mobile technology, known as second-generation (2G) and 2.5G technologies. These technologies provide data connection speeds ranging from 9.6kbps (for GSM and CDMA – Code Division Multiple Access – technologies) up to 114kbps (GPRS – General Packet Radio Service).

M-commerce services that are supported by these technologies are typically low value transactions such as the provision of information like news headlines or advertisements, playing games and making small purchases. Current 2G networks rely on SMS for these transactions to be completed.

[22] Early in 2002, 72 per cent of Australian mobile phone users used SMS, AT Kearney, 2002, Mobinet Index # 4, February 2002, http://www.atkearney.com http://www.atkearney.com

[23] Early in 2002, 19 per cent of Australian mobile phone users had received SMS advertising, ibid.

[24] 178 per cent compound growth to 90 million MMS users by 2007, IDC 2003

[25] Telstra, 2001, *Wireless/work*, October 2001

[26] AT Kearney, 2002, *op cit*.

More advanced networks, for example 2.5G and 3G, could facilitate more advanced m-commerce services, including location-based services, Internet access, remote control of home networks and security systems and mobile banking.

Finding 4: In the short to medium term, m-commerce services are likely to be delivered using existing 2G and enhanced 2G (2.5G) technologies and networks. This could result in the majority of transactions being reliant on SMS and text-based information between consumers and businesses.

The Next Generation Networks

The emergence of next generation networks (NGN) and services in Australia is evident in the data and voice over packet services provided to the corporate and business sectors, and services provided by Internet Service Providers (ISPs). These networks are expected to support increasingly complex applications and increased collaboration between computing and telecommunications providers to provide converged, seamless wireless services across multiple platforms, in turn creating opportunities for innovative applications and services.[27] Mobile commerce services are expected to expand with the availability of NGN networks.

The NGN value-chain is more complex than traditional telecommunications services, particularly at the services provision end. This may open the way for other providers to be involved in the delivery of NGN services, beyond the traditional vertically integrated carriers. Maintaining any-to-any connectivity for voice telephony and developing any-to-any connectivity for text or other services may require interworking arrangements between legacy systems and NGNs.

Given their focus on broader social and economic outcomes, the high-level policy objectives of the current telecommunications regulatory regime are not likely to change significantly in the face of technological change and the rollout of NGNs. However, as more people use these services and the community builds expectations of quality of service, policies that take consumer requirements into account are likely to be needed.

At this time, the telephony service remains a key service and its integrity needs to be safeguarded for the foreseeable future. The increasing complexity of services may give rise to a need for additional consumer safeguards and the ACA is examining these issues to ensure that the long-term interests of end-users are protected and that technological neutrality is preserved as far as possible.

NGN services

Telstra launched *Telstra Mobile Loop* to Australian consumers in March 2003. Mobile Loop is delivered on Telstra's upgraded CDMA network. Customers are able to download applications to their handsets. Ring tones, screen logos and SMS are still the main fare, with picture messaging (an MMS application), games, email, chat, and news or entertainment alerts added to the menu.

Optus has launched some services on its 2.5G GPRS network. Subscribers can access Internet search sites such as Google and Australian news sites that have been customised for wireless users. Optus is currently the only Australian carrier to allow mobile Internet access outside of a 'walled garden' of selected content. Optus plans to trial 3G services in Sydney from July 2003, but has said that it has no plans to launch 3G services for several years from that date.

Vodafone's *live!* provides m-commerce services on GPRS networks in Australia and New Zealand. Subscribers can select from features such as picture messaging, games, ring tones, content and information services, and email.

Telecom New Zealand offers *027* services on Telecom Mobile's upgraded CDMA network. Features include video messaging, email, mobile Internet access via WAP (Wireless Application Protocol), and video games.

Hutchison launched its 3G service, *3*, in April 2003. Hutchison's wideband-CDMA network has the technological capacity to offer the most advanced mobile services in Australia. However, Hutchison is rolling out its m-commerce services slowly. *3* currently offers live video calls, games, information services, news content and wireless Internet access. *3*'s relatively low introductory pricing, presumably intended to generate a high rate of initial adoption, has surprised many in the industry. If *3* does have a fast take-up rate, this may force other carriers to lower their own prices, which could accelerate m-commerce adoption in Australia.

[27] Australian Communications Authority, 2003, *Next Generation Networks: An ACA Perspective on Regulatory and Policy Issues*, ACA Contribution for Discussion ACIF NGN FOG Regulatory & Policy sub-group meeting, 20 May 2003

3G networks are currently being rolled out by a number of operators. Because these are starting from scratch, and given the tremendous cost of rollout, these services are likely to initially only be available in the larger cities.

The primary benefits of 3G lie in the way that information is presented, with the technology allowing for more lengthy documentation to be delivered to a consumer, web links to real-time information and pictures, sound and video capabilities. However, industry analysts agree that the availability of new generation technologies is only one of the drivers for m-commerce adoption.

Already, plans for fourth-generation (4G) mobile communications networks are being developed. This technology is expected to reach commercial markets by the end of this decade (2008 – 2010).[28] In 2000, NTT DoCoMo announced it would invest over $200 million to develop 4G. Korea and Japan, in 2002 agreed to cooperate in establishing a 4G mobile phone network between the two countries. The availability of 4G services for the mass market is, however, a long way off.

Finding 5: Third generation (3G) mobile networks, expected to be offered in Australia in 2003/04, are likely to drive the development of a wider variety of m-commerce applications.

2.6.2 Cost of m-commerce services

While it has been predicted that 3G technology could increase the availability of m-commerce services, there is some criticism that the cost of developing 3G networks, and attempts by telecommunications operators to recoup these costs, may mean that m-commerce services could be far more expensive than their more traditionally offered counterparts. European network operators paid between $US500 and $US600 a customer for 3G licenses, requiring them to double the revenue earned from each customer just to recover their costs. In Australia, the $1.1 billion paid for 3G licenses by Australia's successful 3G bidders has been estimated to be substantially less than the price paid by European operators on a per customer basis. However, there is still expected to be a gap between what operators need to charge to recoup their costs and what customers are willing to pay, which could put pressure on network operators. Market research performed by Gartner Research has indicated that, in general, customers would be willing to pay only a 20 per cent premium for 3G services.[29]

Transaction fees are also likely to have an impact on merchant acceptance of m-commerce and their willingness to offer consumers this alternative method of payment. Fees could be charged both by telecommunications network operators and financial providers. Many merchants are small and medium enterprises and do not like the idea of paying for a service when there are acceptable, free substitutes around, such as cash. Costs may be passed on to consumers. The extent to which merchants or retailers add additional costs to a transaction to cover their own costs is a factor which could also impact on consumer acceptance of m-commerce.

The recent experience in Australia where retailers are now allowed to pass on the costs of credit card transactions may provide some indication of how consumers are likely to respond to additional charges and fees associated with the new technology. Lower transaction costs are favoured by consumers, merchants and financial institutions.

Finding 6: The cost of 3G technology could inhibit consumer uptake, at least in the medium term.

2.6.3 Availability of new services

Despite the hype, there are currently only limited m-commerce services available to the consumer market. In the current stage of development, transactions with a value of less than $10 to $15 per purchase are dominating m-commerce services. This includes the provision of information such as news headlines, share and sports alerts or entertainment such as games, ring-tones and pictures that can be downloaded onto the phone itself. From an operator's point of view, these are *telecommunications-related products* that are relatively risk-free, since they are low value transactions that do not require any physical delivery of products.

A number of operators are currently piloting the delivery of what can be termed non-core *telecommunications products* where customers can purchase products from third parties that are not directly related to the phone

[28] Budde, P. 2003. *fromPaulsDesk*, http://www.budde.com.au. Accessed 29 July 2003

[29] Bennet, B. 2002, High delivery costs stifle realisation of 3G promise, *The Age*, 21 May 2002, p 5 NEXT

or telecommunications service. These services involve relatively low-value micro-payments and can range from purchasing information updates, like football scores, to exploring instant transactions such as paying the toll for the Sydney Bridge or Citylink or paying for parking.

Services that involve the purchase of a physical good, such as the "Dial a Coke" trial, are currently being trialed in Australia and are likely to continue to be developed. The "Dial a Coke" trial has recently seen the launch of approximately 20 m-commerce-enabled vending machines around Australia, including train stations and shopping centres. With a phone call, you can connect to the machine, order a drink from the menu that appears on the phone and have the drink added to your phone bill.

Over time, development of m-commerce services is likely to follow a similar path as Internet services. As consumer confidence grows, m-commerce applications may expand into more complex, higher value transactions. Ticket purchasing, bill payments, charitable donations, subscriptions, music and DVD purchases are likely to be possible using mobile technology.

Some examples of m-commerce services currently available or in development are provided in Appendix 1.

Finding 7: The market for mobile services and transactions is expected to be driven by early adopters over the next 12 months, with the mass consumer market not contributing significantly to adoption until there is a variety of content and applications available, and the costs of services and the required technology decrease.

In the short to medium term, m-commerce services available to the consumer market are likely to be limited to those which represent relatively small values (micro transactions under $20). The purchase of telecommunications related products, e.g. ring-tones and games, is anticipated to continue be popular, with limited niche services developing to enable transactions for non-telecommunications products.

2.6.4 Compelling content

There are a number of divergent opinions about the sort of content that will drive the uptake of m-commerce. One view is that the content transaction could become closely related to the business of the network operator. It has been estimated that, by the end of 2003, mobile operators could derive more revenue from content than third-party service providers. Ovum research have made an assessment that operators may attract a 61 per cent share of global revenue for content, to a total of US$22.3 billion. By comparison, non-operators are expected to earn just US$15.5 million from mobile content at end 2005. Ovum have predicted a far more aggressive approach to developing and securing content by network operators, noting that their previously cautious approach meant that they "missed the boat" with the first wave of content, notably ring-tones and adult content.[30]

Another view is that content could diversify and that the digital content market can enjoy strong growth by 2005. Some industry players consider that web content and information services are likely to only be successful if they are time critical, require mobility and are suited to the platform. Others see a broader role for content, but there is general agreement that the challenge for the market is to find enough "killer" applications to make an appealing offering. At the same time, the content must be available across platforms and networks to attract high levels of users.

The most recent trend is the capacity for mobile phones users to take and send photographs. Phones are being sold with built-in mini digital cameras and a storage capacity of up to 10 million bytes (10Mb) of digital pictures. Content delivery will take advantage of multimedia features on mobile phone handsets.

Finding 8: To date, it appears that the lack of compelling content, the limited applications and services and the small number of providers are predominant factors inhibiting the uptake of m-commerce.

[30] http://wwwlepaynews.com/newsletter/epaynews228.html

2.6.5 Hardware and handsets

The end-user component of the hardware sector includes the equipment owned and operated by individuals that provide access to mobile telecommunications services. This includes handsets, motor vehicle hands-free kits, earpieces and mobile phone cases. In 2002, almost 4 million handsets were sold in Australia and in the first quarter of 2003 more than one million handsets were sold.[31]

With an already significant penetration rate, it is expected that mobile phones are likely to be the primary access platform for m-commerce services in the short to medium term. Although the available technology provides a basis on which to promote the uptake of m-commerce, this technology also has a number of limitations. The most obvious of these are the small screens, which limit the amount of text that can be viewed, and keyboards that offer only a dozen or so keys to enter letters and words. With the current trend towards smaller handsets, the limitations on conducting m-commerce transactions through conventional data entry are becoming more pronounced.

At the same time, there are new mobile phone handsets being launched that offer a range of other functions, including the ability to download advanced data such as photographs and animations. The screens are bigger and of higher resolution, the quality of sound is better and batteries have a longer life span. The degree of effort associated with making a transaction on mobile services, or ease of use, could also be a major factor in uptake.

Other wireless devices are also becoming available. This includes personal digital assistants (PDAs) that offer advantages over mobile phones, such as larger and multicolour screens, easier data entry and use of richer graphics. Devices such as PDAs and mobile phones could converge to offer new equipment models that are conducive to m-commerce. Wireless laptop computers and smart appliances and devices could also progressively become available as the market for m-commerce services and wireless technologies becomes more advanced.

To use 3G, the current generation of mobile phones may have to be replaced with new handsets that support multimedia, including streaming audio and video, offer improved data storage capabilities and create the opportunity for an uninterrupted mobile Internet connection. The cost of the hardware is likely to decline over time; however in the short to medium term, the cost of new handsets is likely to be prohibitive for the mass consumer market.

Finding 9: Mobile phones are likely to continue to be the primary piece of equipment to conduct m-commerce transactions in the short to medium term. In the longer term, new handsets and equipment are expected emerge to enable more complex transactions, including payment services.

2.6.6 Consumer sentiment

While very little research has been undertaken in Australia, there are a number of international studies that examine how consumers are likely to respond to emerging m-commerce services.

In Europe, a survey of consumers found that the most desired m-commerce services included information and news retrieval and banking. However, as shown in the following table, even within Europe, there are considerable differences in demand. From this it can be assumed that cultural factors may be a significant factor in consumer demand and that sentiment in the Australian market is likely to differ.

Table 2: Desired Mobile Services in Europe[32]

Services	Germany	Greece	Finland
Banking	10.9	8.4	13.2
Shopping	1.8	2.6	1.3
Entertainment	7.2	7.9	37.1
Information & News	19.7	15.4	15.5
Travel Booking	3.6	3.5	2.0
Ticket reservation	2.9	3.6	4.7
Email	31.5	15.3	10.9
Other	3.9	0.6	0.8
None	18.1	42.2	14.1

[31] Allen Consulting Group, 2003, *op cit*.

[32] Vrechopoulos, A. et at, 2002, *Critical Success Factors for Accelerating Mobile Commerce Diffusion in Europe*, 15th Bled Electronic Commerce Conference, E-Reality: Constructing the eEconomy, Bled, Slovenia, June 17-19 2002

A recent trial of five m-payments projects in Singapore that involved carriers, banks, merchants and technology companies revealed a number of apparent consumer preferences. The trials, involving 7,000 consumers, concluded that:

- consumers are likely to use m-payments for: bill and fine payments, Internet content and application purchases, vending machines, top-up of prepaid accounts, person-to-person payments and goods with limited shelf lives, and
- consumers prefer credit for m-payments, they are not too keen on buying new handsets and those aged 20-40 appear the most receptive to m-commerce.

Evidence and informed opinion in Australia is conflicting. Paul Budde, a telecommunications analyst, has argued that people may not use m-commerce services because they prefer their mobiles for voice and text communication. The uptake of WAP phones that enable access to the Internet supports this view. WAP has not been successful in Australia, with a small penetration of WAP-enabled handsets and 5 per cent of people with WAP actually using the features. The main reason respondents give for their failure to date to use the WAP connection to the Internet is a general lack of interest or perceived need to use their handsets for anything other than making calls.[33] Cited deterrents to more extensive use include a lack of comfort and ease of use, worries about security of data and the costs of equipment and service.

Analysis of data compiled by AT Kearney similarly shows that enthusiasm for m-commerce has dwindled since 2000, when 29 per cent of mobile phone customers intended to use it, to 2 per cent in mid 2003.[34] By comparison, AMR Interactive has found that 10 per cent of mobile phone users are interested in banking with phones.[35]

One point raised consistently in the research is that m-commerce is not likely to replace cash. It has been argued that consumers will only accept a new payment system if there is something new and/or compelling to buy that cannot easily be charged for through existing solutions. Acceptance of m-commerce is likely to be slow and it first needs to prove itself useful to pay for services not yet served by other payment solutions.[36]

Finding 10: There is currently little data on the type of m-commerce services that would appeal to Australian consumers.

2.6.7 Integrity of transactions and trust in services

One of the key factors that could significantly affect the uptake of m-commerce services is the extent to which these services offer a reliable alternative to existing options. While m-commerce may, for example, offer a convenient alternative to carrying cash for parking meters or snack foods, or as an alternative payment option, it may not attract a customer base if it cannot be trusted as a medium over which to conduct these transactions.

The trust relationship is built on a number of factors, including the security of the transaction and the customer's personal details and the relationship between company and customer. It has been argued that the uptake of e-commerce using the Internet and home PCs is well below expectation because this trust relationship has not been successfully established and the use of security technologies lags behind latest best practice (see, for example the UK National Consumer Council E-commerce and Consumer Protection, Consumers - real needs in a virtual world 2000). System providers need to be convinced that the technology offers a level of security that reduces the risk of the transaction to a level where the consumer and the merchant can be covered for any fraudulent payment.

Secure online transactions require a method of protection that delivers:

- authentication – ensures the user is legitimate
- confidentiality – the data must be encrypted to ensure it is not able to be read
- integrity – ensures the data is complete and unchanged, and
- non-repudiation – the transaction cannot be repudiated.

There are currently a number of projects being undertaken by industry to enable the secure authentication of

[33] AT Kearney, 2002, *op cit*.

[34] Lia Timson, 2003, Phones that make you go mmm, *The Age*, 9th September

[35] *ibid*.

[36] Ovum, 2002, *op cit*.

merchants and consumers on wireless devices. Developers are looking at biometric systems, including voice, iris and fingerprints as payment authentication methods. However, as noted by the ACA, progress on this front is being slowed by a lack of agreement on standards across industry and cost factors.

However, credit card issuers say that m-commerce implementation depends on factors beyond consumers' trust in the technology.

Finding 11: Development of m-commerce appears to be impeded by a lack of adequate security to ensure integrity of transactions.

2.6.8 Payment and billing systems

The availability of technology to support payment systems has often been identified as one of the factors limiting the widespread uptake of m-commerce. However, in reality the ability for consumers to access bank accounts to pay for goods and services using a mobile phone is already available. The key issue is that, to date, no standardised, widely adopted mobile payment system has emerged.[37]

A number of payment models are expected to be able to support m-commerce transactions and existing billing and payment models have already been modified to handle purchases from mobile phones. New systems are also being developed by operators and financial service providers anxious to use the new m-commerce platform for goods and services transactions.

Carrier billing

The starting point for enabling m-commerce payments has been the ability to charge payments to existing telephone accounts. This approach has been adopted for micro-payments, with telecommunications operators billing on behalf of third-party content providers. This model has been successfully implemented for both post-paid and pre-paid mobile services. It is already operational for the purchase of ring-tones and information services.

This payment option is likely to continue to take precedence in the short term and could represent an important billing option particularly for smaller payments. With their infrastructure and billing relationship with customers already in place, operators have a considerable advantage over financial institutions and service providers for micro-payment charging.

However, rather than being a true mobile payment (m-payment) solution, this has been defined as an m-billing solution. This is the starting point for the Australian m-payments market, but finance providers agree that it is unlikely to be the final answer. In the same way as Bpay, the m-payments solution is likely to continue being modified as standards develop. With a common technology, financial providers could compete on price and features without confusing customers, as Bpay operates today.

Credit card payments

M-commerce services are likely to provide the opportunity to pay from a credit card or debit account. This could be similar to what is already offered through fixed line phones, including making purchases or paying bills. Credit/debit card or other bank details could be entered and transmitted to the service provider over the phone via SMS. An alternative could be that a consumer makes an arrangement with their bank and a merchant for all purchases being made from a particular phone to be charged to a nominated account. While this would eliminate the need for sending credit card details, it is likely that consumers would prefer to have the same banking choices that are currently available with EFTPOS, such as using different savings or credit accounts for different transactions.

One interesting market development is currently being trialed by VISA where phone subscribers can download a soft version of their credit card details or insert a SIM-size chip into special m-commerce phones. These transmit payments to infra-red ports attached to terminals at selected merchants. While this could evolve to be a niche m-payments system, the issues of interoperability are likely to limit its attractiveness as a payment option.

Direct debiting from bank accounts

The industry is also examining systems that enable payments to be made directly to a merchant from a phone. To undertake the transaction, a personal identification number would be entered on the phone to authorise payment for specific services or goods. To be effective,

[37] van Heijden, Han, 2002, *Factors Affecting the Successful Introduction of Mobile Payment Systems*, Paper presented at the 15th Bled Electronic Commerce Conference: eReality: Constructing the eEconomy, Bled, Slovenia, June 17-19, 2002

however, this would require service agreements to be made between banks and telecommunications operators, as the mobile handsets could effectively become a personal EFTPOS terminal for a customer. The extent to which this might lead to proprietary arrangements, where consumers only have one choice of banking service depending on the arrangements put into place by the telecommunications providers, is an issue that could impact on uptake.

The concept of electronic person to person payments has been developed to support secure electronic payments between individuals. The online payment service, PayPal, is now being adapted for mobile phones and would allow users to use their mobile to pay a bill or account, with the amount being charged to a credit card or bank account.

Stored-value phones

The third payment model that could underpin m-commerce transactions is the smart-phone, where money can be electronically loaded onto the SIM card in the phone and used by a consumer to make purchases.

The telecommunications operator who manages the account for the phone would be billed by the merchant. This shares some similarities with both the way existing prepaid phones work and the carrier billing payment model (see above), as the process would not necessarily involve a financial service provider acting as a separate party in the payment process. While this process is likely to address some security issues, and would not require payment details to be transmitted over the network, it raises other issues, particularly for the amount of value a mobile phone can represent for a consumer.

In Europe, non-financial institutions including ISPs and mobile network operators are looking to launch e-money schemes, where a cash value is stored on a PC, smart card or mobile phone. Companies are already developing chips containing credit card information that can be inserted into mobile phone handsets.

This model is more likely to support micro-payments rather than macro-payments.

Table 3: M-commerce payment models

	Carrier based billing	**Existing bank based payment services**	**Direct payment from phone**	**Stored value cards**
Ubiquity	Generally carrier/network specific. Carrier must have a billing relationship with the customer	Can be used over any network with the customer of any bank	Generally carrier/network specific	Can be used over any network with any merchants
Main target market	Micro-transactions – low value, low risk	Medium to high value transactions	Medium to high value transactions	Micro-transactions – low value
Examples	Airline tickets, shopping	Information based services, ring-tones	Paying a bill, making purchases	Information based services, ring-tones

Finding 12: Over time, mobile payments are expected to evolve from simple payments for digital content and commerce to complex integrated handset, bank and operator payments.

It is anticipated that higher value m-commerce services supported by advanced billing or payment infrastructures will be available, however, these are not expected to be taken up by the mass consumer market in the short to medium term.

2.6.9 Relationships in the delivery of m-commerce services

The delivery of m-commerce services is likely to involve a series of relationships between different sectors of the value chain. The following provides a brief snapshot of the various players expected to be involved in the delivery of m-commerce.

Telecommunications network operators

Telecommunications network operators, known as carriage service providers (CSPs), are those companies that own the infrastructure over which m-payments can be conducted. CSPs are defined as suppliers of telecommunications services to the public using carrier network infrastructure. In 2002, 13 CSPs operated in Australia. The three major operators who own and operate infrastructure for mobile services are household names: Telstra, Optus (Sing Tel) and Vodafone. These three operators account for 97 per cent of the mobile revenue in Australia. Although Telstra still has the largest market share, Optus and Vodafone are continuing to grow.

With the introduction of 3G services, and as a result of the 2001 reallocation of spectrum for mobile services, there are a number of new operators that are in the process of rolling out their own network infrastructure to support the delivery of 3G services. Although network owners are the most financially exposed operators in the industry, their market positions are secure because networks are device-neutral and attract traffic regardless of which mobile devices prove most popular.

In developing ways to increase the ARPU, telecommunications network operators are likely to be dominant players in the provision of m-commerce services. They already own and operate the essential platform for transactions and possess the technical expertise in and experience of handling payments, specifically micro payments. They also have the capacity to provide additional services to their large and growing customer base through their current billing and accounting infrastructures. Operators are looking to make their overall services more attractive by providing useful content, hence the trials for making soft-drink purchases and paying for parking tickets.

M-commerce offers telecommunications operators the opportunity to move away from providing simply the communications channel to providing the financial service as well. However, from the consultation process, it appears that operators are unlikely to move into provision of full-blown banking and financial services and would instead be focused on developing billing systems and encouraging consumer confidence in micro-payments through providing adequate levels of security. These payments require little risk management, but with larger m-commerce transaction values, traditional financial institutions would have the advantage over mobile operators.

Hardware providers

Handset manufacturers could play an important role in supporting m-commerce and are already working to keep pace with network operators. Their market position has been supported by the willingness of network operators to subsidise handset purchases in order to generate traffic, but their position in the market is less secure because of the competition in the market for m-commerce devices.

In order to ensure their longevity in the market, handset manufacturers are focusing on developing more direct relationships with consumers. It appears that the focus is currently on developing new devices with extra functions, such as digital cameras, hand held game devices and music players.

Resellers

In addition to the operators, the mobile market also comprises mobile service resellers, or virtual mobile network operators (VMNOs). Resellers are also considered to be carriage service providers in the regulatory sense. Examples of resellers in Australia include AAPT, Austar, Boost and Primus. Resellers are distinguished from CSPs because they do not necessarily own network infrastructure or have a spectrum allocation. They purchase end-to-end mobile

services from the mobile network operators and bill and support customers in their own names.[38] VMNOs are able to issue their own SIM cards and are likely to offer m-commerce services to their existing customer base in an attempt to gain market share and establish their own relationships with content providers.[39]

Financial service providers

'Traditional' providers of financial services, such as banks and credit unions, 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.[40]

M-commerce provides a new channel for customers to access banking services. The provision of a gateway service allowing users on any network to access their bank account details would ensure that banks retain the customer interface for payments.

There has been increasing competitive pressure on traditional financial providers from the telecommunications sector, which is well-placed to provide additional services to its large customer base. This is particularly important as the financial sector's ARPU is declining and telecom operators are looking for ways to increase their own ARPU.

It has been predicted that financial service providers could seek a more direct role in the provision of payment services to carriers and third-party m-commerce players. Off the shelf packages are available on mobile networks for Virtual Mobile Network Operators (VMNOs), companies that offer mobile services to customers using a third party's network. In functional terms, this would mean that banks would become very much like service providers, managing the customer relationship and using the network of operators to resell network space.

Mobile payment providers

Mobile payment providers are also emerging specifically to deliver m-commerce services. In Australia, a group called Unidex has developed a technology that allows credit card payments to be made via a mobile phone. In partnership with Telstra, Unidex will be offering its model to businesses around Australia.[41] New payment providers could emerge as the market develops.

The introduction of Special Credit Card Institutions (SCCI's) licenses, as a result of the reforms being made by the Reserve Bank of Australia[42] could enable new organisations to enter into the credit market, and open the way for telecommunications operators to also offer credit to consumers for m-commerce.

Retail merchants

Retailers offer mobile services to end-users on behalf of network operators/CSP's. Customers can purchase mobile telecommunications hardware and services from either specialty outlets or outlets that sell mobile telecommunications hardware and services as part of a broad range of products.

Retailers are likely to view m-commerce as offering a further avenue to market and sell goods. To date, retailers have overlooked m-commerce in the belief that their products may be unsuitable for the mobile channel. However, as technology advances, the range of m-commerce products may grow.

While collaborative relationships between service providers and retailers to attract customers are likely to emerge, the ability to make any purchases of goods or services or content over any network is likely to be the most important factor for a consumer and retailers are unlikely to want to lock themselves into individual relationships with service providers.

Content providers

Content providers have started developing services for mobile users, but to date, have shown little interest in m-commerce. This is partly explained by the lack of an established billing relationship with users.

The predominant content to emerge to date has been games and entertainment applications that can be

[38] Allen Consulting Group, 2003, *op cit*. p.13

[39] *ibid*. p.14

[40] Yorulmaz, T. and Ragas, D. 2002, The m-commerce roadmap, AFP Exchange, Bethesda.

[41] Nicholas, K. 2002, Telstra to market mobile credit pay units, *Australian Financial Review*, Saturday 5 October 2002, p. 17

[42] Reserve Bank of Australia, 2003, *Reform of Credit Card Schemes in Australia*, Media Release 19 September 2003, http://www.rba.gov.au/MediaReleases/mr_03_12.html

downloaded and played on a phone rather than real-time services. However, as m-commerce services continue to gain popularity, content that can be delivered to a mobile phone could expand beyond games and simple information services. This is likely to occur when content providers can support interoperable services (across all operators and the Internet) and provide quicker ways to market by offering more transparent fee models.[43]

In the race to attract customers, network operators and handset manufacturers are attempting to develop relationships with content providers. In 2002, the United States witnessed a number of these partnerships, such as the one between Verizon Wireless and BREW[44] content providers. The service launched by Verizon enables their customers to download games, entertainment and information onto their mobile phones. The applications are only accessible through BREW-capable phones and Sony has announced that is developing games based on the BREW platform.[45]

Despite the race to develop content, these proprietary relationships may not last as consumers demand to access the full range of products from different service providers across different platforms. Furthermore, content providers could come under pressure to develop sites that cater for all kinds of devices. It may not be sufficient to deliver web-based information over mobile phones, since this content is primarily developed for a typical computer screen and is usually only accessible by clicking through several navigation layers. Content developers may need to ensure that content is more easily accessible and is tailored for different devices.

It has been suggested that m-commerce services are likely to focus on content that is simple, time sensitive and focused on providing information for impulse buying, share-trading and auctions. For content providers, including merchants, it is expected that mobile and PC content will converge so that marketing messages delivered to each kind of device can reinforce each other.

Finding 13: In the short to medium term, it is estimated that the key industries in the m-commerce value chain will develop partnerships to deliver m-commerce services rather than attempt to extend their reach into the provision of new services.

2.6.10 Operator models

In the traditional model, banks own the relationship for financial transactions, telecom providers own the relationship for the communications and the content provider has a separate relationship with the customer for the delivery of content. This model is changing with the convergence of services and owning the customer relationship could prove to be a challenge for all elements of the value chain.

For 3G operators, three alternatives have been identified[46]:

- walled garden: Prevents or discourages users from accessing content not affiliated with the network operator
- open access using another portal: Allows users to access any website that is written in a language that is compatible with their access device (e.g. WML for WAP phones and HTML or Java for i-Mode phones), and
- open access using operators portal: Allows users to access any website that is written in a language that is compatible with their access device, although access is typically via the operators portal.

Carriers have been drawn to the walled garden approach in the short term. This is partly because, at present, consumers like to see items on their phone bill. In the long-term, however, such a structure may discourage development of content and slow uptake, and carriers are unlikely to sustain this model. Consumers are likely to expect a wide range of content that would be beyond the ability of one organisation to provide. A likely future structure could see a combination of operator portals and open access, with carriers providing billing services to third parties.

[43] Ovum, 2002, *op cit*.

[44] BREW (Binary Runtime Environment for Wireless) is software developed by Qualcomm for designing and deploying wireless content

[45] Ed, 2002, Mobiles call on gamers, MX, Thursday 6 June 2002, p. 21

[46] Schema, 3G in Australia, , http://www.schema.co.uk/Assets_pubs/ 3G%20in%20Australia.pdf

While operators have initially developed relationships with individual suppliers, it is thought that operators could be moving forward to an open model where anyone can supply goods using the different networks.

Finding 14: It is unlikely that any one player in the market is going to maintain dominance in the relationship with customers into the future. Cooperation between network operators, financial providers and content providers will be key to delivering m-commerce services.

2.6.11 Interoperability and standards

There appears to be universal agreement between key m-commerce stakeholders that consumer use of m-commerce services could be impacted on by the ability of merchants, content providers, financial institutions and networks to come together to develop a ubiquitous system with interoperable components that offers a secure and trustworthy environment for transactions. The lack of ubiquitous standards and a glut of industry forums proposing different methodologies could limit uptake of m-commerce.

The issue of interworking and interoperability of equipment is a key consideration of the ACA in its m-commerce discussion paper. As noted by the ACA, a number of standards groups, industry alliances and consortia are working towards establishing standards for m-payments and m-commerce. The ACA noted that, until recently, m-commerce standardisation had been fragmented, contributing to the failure of m-commerce to achieve the level of acceptance that had been anticipated by analysts two years ago. The number of projects that are being undertaken by different forums is of concern, particularly since most of the forums represent a specific interest group. Discussions across the various industry groups that are involved in the delivery of m-commerce suggest that uptake would depend on how well the groups work together to promote the services and to provide a solution accessible by all, regardless of carrier, handset or bank.

Interoperability is a key issue for messaging via MMS, which is likely to be the most popular feature of 2.5G and 3G services in the early years. Originally, MMS could only be sent between users on the same network. However, from August 2003 Vodafone, Optus and Telstra subscribers of the major network operators have been able to send full colour images, video and sound to each other. If a handset receiving the MMS message does not have this capability, an SMS message is sent to the receiving party allowing them to check the message via the Internet instead.[47] The issue of international MMS interoperability, unlike SMS, still requires attention.

Similarly, there appears to be greater co-operation between mobile operators to enable the use of standardised payment systems and, therefore, greater transparency in the market. In early 2003 a number of operators launched the Mobile Payment Services Association (MPSA) initiative. The MPSA is expected to launch two payment services next year. The first enables the purchase of low-priced items through operator-managed accounts. The second allows users to register their credit-card details in advance, and then pay using their personal identification numbers.[48]

Finding 15: The lack of current standards for m-commerce and m-payments, and the proliferation of activities that are taking place in the race to create solutions may be hampering the development of m-commerce services.

Consumers are likely to expect fully interoperable m-commerce services, rather than accepting the limitations inherent in proprietary infrastructure. Operators and banks are working to develop standards, recognising these as critical in promoting the development of m-commerce services and uptake among consumers.

[47] Optus Newsroom, 2003, *A picture tells a thousand words*, 12 August 2003, http://www.optus.com.au. Accessed 22 August 2003

[48] Ed, 2003, Phone me the money, *The Economist*, Mar 13th 2003, http://www.economist,com/displaystory.cfm?story_id=1633316 Accessed 20 April 2003

2.6.12 Regulatory framework

From all perspectives, there is concern that the current m-commerce regulatory framework is inadequate to either support rollout of new services or protect consumers. While this paper aims to focus on the key consumer issues, there are a range of other regulatory issues that may also impact on the rollout of m-commerce services.

In addition to consumer law and trade practices legislation, m-commerce services are likely to be subject to a range of other laws, including the *Telecommunications Act* 1997 (Cth) and the *Radiocommunications Act* 1992 (Cth). Laws governing the provision of finance and banking services are also likely to be relevant, as well as regulations that cover the provision of content, including the *Broadcasting Services Act* 1992 (Cth). There is concern among industry that the complex interplay of these laws may lead to over-regulation or mis-regulation.

Current inquiries into m-commerce

This review is just one of a number of activities currently being undertaken in response to the emergence of m-commerce services.

The ACA is currently examining the regulatory framework as it applies to m-commerce, with a particular focus on issues that could impact on the development of the m-commerce industry. A public discussion paper, released in August 2003, provided information on m-commerce trends and issues. The objective of the paper was to seek comments on the applicability of the telecommunications regulatory regime to m-commerce, and develop a view of whether, and how the introduction of m-commerce could affect the ACA's regulatory responsibilities.

The ACA received submissions from a number of interested parties that confirmed the view that m-commerce is a growth area, and raised a number of issues that are currently being considered further by the ACA, including consumer issues, regulatory issues, standards and international issues and the regulatory options that exist to deal with m-commerce. This includes regulations, industry codes and guidelines and dispute resolution mechanisms.

The Federal Government's E-commerce Expert Group has also announced its intention to examine m-commerce. It is currently seeking comments on whether and how Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business (BPM) should be modified to ensure its relevance to m-commerce.[49]

Finding 16: The issues associated with the introduction of m-commerce have caught the attention of regulators internationally and in Australia.

A co-operative approach between agencies will enable a full consideration of the issues raised by m-commerce and the development of a regulatory approach that will stimulate the development of the m-commerce industry in Australia while providing suitable safeguards to users.

2.7 Summary

As is the case in most markets where there are network externalities, the acceptance and use of m-commerce by consumers, merchants, telecommunications operators and banks is highly interdependent. Critical mass in one area could certainly impact on critical mass in another.[50]

It has been argued that rather than m-commerce creating a revolution, with users abandoning their usual way of doing things to do them with a mobile phone instead, the adoption of mobile technology to perform transactions could evolve in much the same step-by-step way as the adoption of the PC. The mobile phone began as a telephone, has become a text messaging device and in the future may become a shopping and transaction tool. The growth of e-shopping with PCs is encouraging for m-commerce. An experience with one Internet access device clearly prepares the ground for the same experience with another. But, because of the size and nature of its access device, m-commerce is unlikely, initially at least, to be used for as wide a range of products and services as PC-based e-commerce. It seems best suited for impulsive,

[49] http://www.ecommerce.treasury.gov.au/bpmreview/default.asp

[50] van Heijden, Han, 2002, *op cit*.

[51] AT Kearney, 2002, *op cit*.

hurried buying decisions, where there is no need for elaborate graphics and long lists of options. There is still plenty of scope for creative ideas to extend the range of suitable m-commerce products and services.[51]

Adoption of m-commerce is likely to be driven by user-friendly devices, useful network and vendor services and rich content.

Timely action is necessary to avoid a regulatory vacuum between the current framework and a framework based on next generation networks and services. It is important to act in the public interest but avoid excessive or inappropriate regulation that unnecessarily increases costs to customers or acts to discourage the development of a competitive market.

The issues that currently impact on consumers, such as security, identity and privacy are likely to be issues of importance in the m-commerce market. The current regulatory regime that covers telecommunications services, commercial and financial transactions and the delivery of content using traditional channels could remain valid for m-commerce services. However, there may be other problems introduced with, or specific to, m-commerce that are not dealt with under existing frameworks.

In the converged market, some jurisdictions are looking at the development of a single regulatory regime to cover information and communications services. The UK has already established a single regulator, with the establishment of the Office of Communications (Ofcom). Ofcom will be the UK's new communications industry regulator with wide-ranging responsibilities across the UK's communications markets when it assumes its powers at the end of 2003.

Ofcom will inherit the duties of the five existing regulators it will replace – the Broadcasting Standards Commission, the Independent Television Commission, Oftel, the Radio Authority and the Radiocommunications Agency.[52] Ofcom will also fulfil the additional duties enacted in the provisions laid down in the *UK Communications Act* 2003.[53]

At this stage, greater understanding of the developments and directions the market is likely to take is needed to ensure a responsive and flexible regulatory environment.

It is acknowledged that responding to many of these issues may require the coordinated effort of government and the private sector and could rely on a mix of self-regulation, technological responses and government regulation, across a range of portfolio areas. Players in the m-commerce market, government regulators and consumers all need to take part in any discussions of regulatory frameworks that may be required to support the development of this emerging market.

[52] http://www.ofcom.org.uk/

[53] Government of the United Kingdom, 2003, *Communications Act 2003*, http://www.legislation.hmso.gov.uk/acts/acts2003/20030021.htm

"Section 3 Key Issues"

3

M-commerce consumers are likely to want everything to work just as well in the mobile world as it does in a store. They may want to be able to make m-commerce payments in the same way that they make e-commerce or store payments – easily, quickly, safely and with confidence.

This section of the issues paper focuses on identifying the potential issues that are likely to arise with the introduction of m-commerce across the following five broad categories:

- Fair trading
- Financial
- Privacy
- Security
- Content

The discussion draws on work already undertaken by the SCOCA E-commerce Working Party in its discussion paper *Online Shopping and Consumer Protection*[54]. It is evident that a number of the issues that could impact on m-commerce have already been identified as relevant to e-commerce transactions. Other general fair trading issues, such as refunds and cancellation policies and issues of currency and price, are also likely to be applicable to m-commerce as they are to online shopping. While these have not been fleshed out in this paper, the E-commerce Working Party would welcome comments on other issues that stakeholders perceive as important for consumers in m-commerce transactions that are not considered here.

The analysis undertaken in this Section provides the basis for consideration about whether there is a need for additional protection mechanisms to be put into place for consumers and, if so, what form these may take.

3.1 Fair Trading Issues

Fair trading issues relate to issues that arise between a trader and a purchaser. When there is no personal contact with the retailer and the consumer is paying for goods before delivery, there are increased concerns about the quality and suitability of the goods, whether they will be delivered on time (or ever), what procedures are in place for refunds and complaints and how the consumer can get in touch with the merchant. These concerns and uncertainties may be magnified when merchants are located in other jurisdictions and when there is reduced ability to access further information due to the limitations of the technology used, such as a mobile phone handset.

3.1.1 Making an informed purchase

Description of the problem

Potential problems may arise in m-commerce transactions that involve purchasing a good, because, as in other forms of distance selling, consumers require more information about products they cannot physically inspect.

[54] SCOCA E-commerce Working Party, 2003, *Online Shopping and Consumer Protection* p.7

Information needs to be clearly displayed to enable an informed decision about whether to make the purchase. The information needs to be understood by people with a wide variation in ages and financial and technical sophistication. Mobile handsets and devices with limited screen capacity may not be able to display enough information to the consumer in order for them to make a decision about a purchase.

Knowing the identity of the business, as well as other information such as a contact phone number is also a significant issue in m-commerce. Furthermore, the question of whether a phone number or e-mail address for contacting the company is sufficient is likely to be tested in m-commerce transactions.

For many current transactions, a disclaimer is used to prevent a representation from being considered misleading when read on its own. While websites can use links and pop-up windows to display restrictions clearly, some mobile devices may not have the ability to display a lengthy disclaimer. Disclaimers should not be used in m-commerce representations unless the mobile device can display its contents to the user.

The marketing of financial services over mobile phones could be very difficult in light of the information a provider must obtain about a customer in order to meet regulatory requirements.

Industry approaches to the issue

Discussions with telecommunications carriage service providers indicate that there has not been much thought given to the issue of providing adequate product information. This is probably because current purchases are primarily limited to small electronic products that complement the use of the phone. In considering more complex transactions, where pre-purchase disclosures or disclaimers need to be supplied to a potential customer, the approach has been that this more detailed information will be provided via more traditional mechanisms; i.e., once a purchase is made, consumers will either be sent information about the purchase or directed to a website for more information and to download copies of the contract and purchase.

Guidance as to what information should be included on websites for electronic traders is contained in the *Best Practice Model (BPM) for Electronic Commerce*, which has been developed to provide advice to businesses trading electronically. The BPM recommends that businesses identify themselves and provide sufficient information about a transaction for a consumer to make an informed choice.

Mobile phone accounts are likely to be linked to individual web accounts where further information and receipts can be delivered to customers. However, the extent to which this will be adequate in enabling consumers to make an informed purchase at the time of payment is questionable.

In terms of who will provide this information, it appears that the responsibility will rest with the service provider as distinct from the telecommunications carriage service provider.

Current regulatory protections in Australia

The fair trading legislation in most states and territories covers the information that must be provided to a consumer at the time of sale in relation to particular types of transactions, for example direct marketing, door-to-door selling etc. In Victoria, for all non-contact sales, the *Fair Trading Act* 1999 requires disclosure of the supplier's full business address or telephone number,[55] the total price, postal/delivery charges and the availability of any cooling off rights. Where such cooling off rights exist, they are deemed to be 10 days.

Under Corporations Law every company must be clearly and uniquely identified. A key element in identification is the company name, which must be registered with the Australian Securities Investment Commission (ASIC) at the time of incorporation. A company name must indicate the company's legal status. A company's name must appear on its published documents, negotiable instruments, and documents lodged with ASIC. It must also be displayed at its registered office.

There is a risk of increased breaches of the *Fair Trading Act* in m-commerce if businesses (rather than taking extra care in ensuring the representation is not misleading) fail to provide the required statutory information.

International regulatory responses

In the European Union (EU), a number of e-commerce related directives have been introduced, including the 1997 Distance Selling *Directive and the E-Commerce Directive*.[56]

[55] Fair Trading Act 1999, Non-contact sales agreement provisions (Part 4, Div 3)

[56] IDATE, 2002; Frost&Sullivan, 2000

The *Distance Selling Directive* provides consumers with a cooling-off period (under certain circumstances) and imposes time limits on the provision of goods. Prior to the conclusion of any distance contract, the consumer must be provided with clear and comprehensible information concerning:

- the identity and possibly the address of the supplier
- the characteristics of the goods or services and their price
- delivery costs
- the arrangements for payment, delivery or performance
- the existence of a right of withdrawal
- the period for which the offer or the price remains valid and the minimum duration of the contract, where applicable, and
- the cost of using the means of distance communication.

This information must comply with the principles of good faith in commercial transactions and the principles governing the protection of minors. In the case of telephone calls, the caller's identity and commercial purpose must be made clear at the beginning.

The Directive aims to provide consumer protection for contracts concluded at a distance, including via the Internet. The Directive mandates that the consumer receives prior information concerning the main terms of the contract. Member States were required to implement the Directive into law by 2000.

The central element of the legal framework for e-commerce in Europe is the *E-Commerce Directive* of May 2000. The Directive covers all services conducted electronically. The main principle of the *E-Commerce Directive* is to allow electronic contracts to be used as an alternative to physical contracts. However, exceptions apply to some specific contracts such as those relating to family and probate law. The Directive stipulates the country of origin principle for e-commerce within the EU states and provides that the law of the country in which the provider is resident shall be applicable to trade via the Internet.[57] A central point of the Directive is the question as to which law is applicable to commerce via the Internet in the case of inter-jurisdictional transactions. The *E-Commerce Directive* may extend to m-commerce services.

The Directive includes a liability exemption for intermediaries where they play a passive role as a mere conduit of information from third parties and limits service providers' liability for other intermediary activities such as the storage of information (i.e. caching). The Directive also imposes certain specific requirements with respect to advertising and marketing online. These commercial communications must not be misrepresented as something else and must identify their source.

Members of the EU are expected to adopt the key provisions in the *E-commerce Directive* into their own legislation; however, the extent to which this has occurred to date appears patchy. In the UK, the Department of Trade and Industry (DTI) implemented the *Electronic Commerce Regulations* based on the Directive in mid-2002. The Regulations are designed to clarify what information e-tailers and other online businesses must supply to customers, including liability issues.

In 2002, the EU adopted a further Directive concerning the distance marketing of consumer financial services, recognising that the intangible nature of financial services makes them particularly suited to distance selling. The Directive was introduced to increase consumer confidence in the use of new techniques for the distance marketing of financial services. Under the new Directive, consumers must be supplied with information regarding the identity and business of the supplier, the characteristics of the service and the terms and conditions of the contract. Consumers have 14 days to withdraw from the contract without penalty, and for specific products such as life insurance, this is extended to 30 days. Unsolicited services, where services are offered without a prior request from a consumer, are prohibited. The absence of a reply does not constitute consent.[58]

In May 2001, Canadian Federal, Provincial and Territorial Ministers responsible for consumer affairs approved a new approach to harmonise consumer protection legislation in electronic commerce. A common template was approved

[57] E-commerce Law in Europe, e-gateway, http://www.e-gateway.de/recht/ec_law_in_europe.cfm accessed 6 October 2003

[58] European Union, Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, *Official Journal of the European Communities* 9/10/2002

which covers contract formation, cancellation rights, credit card chargebacks and information disclosure. All this information must be disclosed in a clear and comprehensible manner on one Web page and the contract must be provided to a consumer within 15 days. A number of states, including Alberta and Nova Scotia, have adopted the template.

Key issues for consideration

- **Is current fair trading legislation adequate to deal with m-commerce transactions, particularly considering mobile phone technology?**
- **How will m-commerce service providers ensure that consumers have access to required information (eg. terms and conditions of the transaction) and prove that consumers have agreed to such terms and conditions?**
- **Is a phone number or e-mail address for contacting the company about conditions enough?**
- **Who will be responsible for providing information to a consumer about a product?**
- **Will there be some liability on the carriage service provider or will it be up to the supplier/service provider to provide this information?**

3.1.2 Misleading conduct and disclosures about purchases

Description of the problem

Transactions conducted using m-commerce technology could mislead consumers through the inadequate provision of information about products being sold or through false claims about products. Certain claims made in advertising require that the provider or advertiser provide additional information to consumers about the terms and conditions of the promotions in order to prevent misrepresentation. However, given the size of wireless devices, it may be difficult for consumers to read and understand information disclosures provided through a mobile phone.

Information should be communicated clearly and effectively so that consumers notice and understand it. The issue remains as to how likely a consumer is to take the active steps necessary to be informed.

Industry approaches to the issue

Various approaches that use a combination of different technologies are being considered to deal with providing information to consumers regarding purchases made using m-commerce. It has been suggested that at the time of purchase a consumer will be required to make a call to a centre where they can listen to the full disclosure of terms and conditions. Another option is to place the material on a website that the consumer can visit to confirm full details of the transaction. Contractual "clickwrap" agreements used by many websites have already received some criticism regarding their accessibility and options for redress by consumers. Contractual provisions relating to purchases made using m-commerce are likely to raise the same sorts of issues.

There may be some products and advertisements that are not suitable for m-commerce because the necessary disclosures are so lengthy.

Current regulatory protections in Australia

The consumer protection provisions of the Commonwealth *Trade Practices Act* 1974 (TPA) prohibit unfair practices such as: misleading and deceptive conduct, false representations, misleading statements, harassment and coercion, bait advertising, referral selling and pyramid selling. There are also provisions relating to unsolicited goods and credit cards.

The TPA prohibits a variety of false or misleading representations in relation to goods and services. Under the TPA, it is illegal for a business to falsely represent the price of a good, its availability or origin, its quality or standard, and that it is used by certain people or is approved for use by a certain person. Misleading conduct can include silence if there is, in the circumstances, an obligation to say something about the product. It can include a product claim if the maker has no reasonable ground for making it, or if it should have been qualified.

The TPA is technology neutral and capable of addressing illegal misrepresentations and misleading conduct in any form and via any medium. For example, the ACCC has brought several cases involving e-commerce.[59] The same conduct-based provisions will be applied over time by the

[59] For example, the ACCC has launched action in the Federal Court against *Crowded Planet* and Skybiz 2000, regarding selling practices over the Internet. For more information, see htt://www.accc.gov.au

courts to m-commerce, as cases are brought forward including the technical aspects of mobile transactions.

Fair trading legislation in the states and territories mirror the deceptive conduct provisions of the TPA and also impose positive requirements for certain forms of marketing like direct distance selling. Currently the latter provisions vary between the states and territories. In general there are no current regulatory requirements in the TPA or fair trading legislation specifically directed to m-commerce.

International regulatory responses

Misleading advertising and misleading information in business-to-consumer (B2C) sales appears to be predominantly regulated through generic legislation rather than legislation specifically dealing with distance sales or electronic transactions. The EU's Misleading Advertising Directive covers advertising practices. In May 2003, the EU Commission identified its intention to put forward a single comprehensive ("fully harmonised") framework covering all the pre- and post-sale aspects of B2C transactions, including misleading and deceptive advertising. The new Directive will include the B2C provisions of the Misleading and *Comparative Advertising Directive*.[60]

Key issues for consideration

- **There exists a robust regulatory framework within Australia at both Commonwealth and State and Territory levels prohibiting misleading representations. Should legislation also provide for minimum information that should be disclosed to consumers at the time of making a purchase?**
- **Are proposed industry approaches to information disclosures adequate?**

3.1.3 Confirmation of contracts

Description of the problem

The question of the extent to which a contract made during an m-commerce transaction is enforceable has been raised. There is some concern that consumers may feel unsure about whether the transaction has actually taken place. This is already a consumer confidence problem for shopping on e-commerce sites and this issue may be further magnified with m-commerce.

It would be desirable for consumers to be able to print out a confirmation of every m-commerce purchase. Many commercial websites now follow good practice guidelines and present a confirmation that the transaction has been completed with details of total cost, delivery arrangements and so on. This is not required under the law, but it would be desirable to follow the same practices for m-commerce and clarify situations where unreliable SMS messages are not received by either the consumer or the merchant. It is noted that SMS is a store-and-deliver system with no guarantee whatsoever that the message will get through.

The problem would be whether current mobile phone handsets could display so much information and how a consumer could save or print it. In most handsets this would be virtually impossible. Compliance with any statutory requirement to this effect would not be currently possible.

Current handsets also do not enable consumers to save much data. But, it may be important to be able to save a series of records. The Mobile Payment Forum[61], a cross industry alliance that is examining access and barriers to mobile payments has identified digital receipts and their format and storage as an important area of research. It may be much easier to mistakenly delete or fail to save financial records received through a mobile phone handset than online/offline.

Industry approaches to the issue

It is generally accepted by industry that contract law applies to all m-commerce transactions and that contracts will be honoured where they are agreed upon.

The Australian Direct Marketing Association (ADMA) has recognised that there may be some issues associated with making and fulfilling of electronic contracts. In its Direct Marketing Code, it promotes the development of processes that enable a consumer to:

- identify precisely the goods or services they wish to purchase
- identify and correct any errors or modify the order
- express an informed and deliberate consent to the purchase, and
- retain a complete and accurate record of the transaction.

[60] Directive 84/450 OJL 250 19.9.84 p. 17

[61] http://www.mobilepaymentforum.org/

The code also states that the consumer should be able to cancel the transaction before concluding the purchase.

Consultation with industry has identified the role that industry will play in ensuring that transactions can be tracked, to protect both consumers and traders. Technology supporting m-commerce needs to include a security mechanism to ensure that the transaction cannot be repudiated by the consumer or the supplier. Appropriate standards and regulations will also need to be formulated to ensure the use of payment gateways that store transactions on a host service and provide the user with the ability to review/print transaction details through a web-based interface.

It is expected that m-commerce will, in most cases, be supported by other marketing channels such as e-mail, Internet and printed materials. This information will provide a full explanation of, or directions of where to find, the terms and conditions of the offer, contact details and other relevant information. ADMA has argued that the limitation of the mobile screen is really only a temporary issue given that 3G phones enable scrolling of the screen and links through to a dedicated web page for fuller explanations.

Current regulatory protections in Australia

A contract is the primary mechanism for the transaction of business and there are a number of laws in Australia that cover the formulation and terms of contracts. A contract may be governed by the law of the jurisdiction agreed between the parties or by the law of the jurisdiction imposed by the court. Underlying the common law of contract is an assumption of freedom to contract with any person on any terms.

The law prescribes the general elements of a binding contract, but it does not require a contract to be formed by any particular method or to be in any particular form. The general law of contract does not require that a contract be in writing, but legislation imposes a requirement of writing in some circumstances. Furthermore, in certain circumstances, contracts will not be enforceable against people who are under 18 (minors) or who were mentally disordered at the time the contract was entered into. It is accepted that a contract can be formed by a variety of methods including:

- an exchange of correspondence through the post, by telex or by facsimile
- orally, either in person or by use of a telephone, or
- by completion of a formal document.

A contract is not generally required to take a particular form and may be oral, provided there is no specific statutory requirement for the contract to be in writing

The *Electronic Transactions Act* 1999 (Cth) commenced on 15 March 2000 and is based on the United Nations Commission on International Trade Law's *Model Law on Electronic Commerce (UNCITRAL)*. The purpose of this legislation was to lay a foundation for a national legislative framework for facilitating e-commerce. However, even with this legislative framework, the need to rely on principles of contract law has remained. Most common law principles have been shown to be capable of being adapted to an electronic environment without legislative intervention, but the Commonwealth and State governments moved to end any perceived uncertainty about the application of contractual principles through the enactment of the *Electronic Transactions legislation.*[62]

The legislation takes a light-handed regulatory approach and is based on two principles: 'functional equivalence' and 'technology neutrality'. Functional equivalence means that a paper-based transaction and an electronic transaction should be treated equally by the law. Technology neutrality means that the law will not discriminate between different forms of technology. This is evident in the wide definition of electronic communication, which could include communication via fax, email, the Internet and, potentially, m-commerce.

The legislation contains provisions concerning requirements of writing and signature, production of documents, retention of documents, the time of dispatch and receipt of communications and attribution of communications in an electronic environment. An electronic contract may be formed either through an exchange of email or by completion of a document on an Internet website which is submitted to another party electronically. Common business practice means that both offers and acceptances come into effect when they reach the intended recipient.[63]

---

[62] Christensen S. (2001) Formation of Contracts by Email – Is it Just the Same as the Post?, *QUT Law & Justice Journal*, QUTLJJ 3 2001. http://www.austlii.edu.au/au/journals/ QUTLJJ/2001/3.html#fnB7

[63] *ibid*.

The operation of the electronic transactions legislation (now enacted in each state and territory) plays a crucial role in assessing what is needed to facilitate e-commerce in respect of Uniform Consumer Credit Code-regulated credit. However, it is argued that only the sections of the Act concerning the receipt and dispatch of electronic communications can clearly apply to the formation of a contract. While the sections provide times for receipt and dispatch there is no clear indication of the time at which a contract is formed. This leaves the courts to rely upon contractual principles specifically developed and applied within a paper environment.[64]

Recent amendments to Victoria's fair trading legislation empower consumers to obtain proof of a transaction (receipt) that identifies the name of a supplier, the date of supply, the goods and services supplied and the cost of these. For transactions over $50.00 these receipts are mandatory, and for goods under $50.00 they are provided on request.

International regulatory responses

The EU's *E-Commerce Directive* also complements its electronic signatures Directive by obliging Member States to ensure that their legal system allows contracts to be concluded by electronic means.

Specific to the issues raised by e-commerce, under the EU's *E-Commerce Directive*, when an order is placed, the service provider must acknowledge receipt quickly and by electronic means although the Directive does not attribute any legal effect to the placing of an order or its acknowledgment. Whether a contract has been entered into and at what time the contract has been concluded are issues governed by national law.

Korea's Fair Trade Commission has recently regulated to require telecommunications companies to specify the name of third-party m-commerce merchants on phone bills. This will provide some added protection to consumers in the form of additional information by which to track purchases. This move might also encourage a consumer to go directly to the content provider should any dispute about the purchase arise, effectively removing liability for purchases from the telecommunications service providers.

Key issues for consideration

- **Is it enough for terms and conditions and receipts to arrive later in the post? What about for digital goods?**
- **Should there be opportunities for consumers to reverse an order before delivery and is this covered by existing law?**
- **What remedy do consumers have if they sign an electronic contract and the goods never arrive? Where should the burden of proof lie?**
- **Will Standard Forms of Agreement apply to m-commerce services offered by the carriage service provider?**

3.1.4 Access to redress and dispute resolution

Description of the problem

Where there are problems with a purchase from a local store, a consumer can talk face-to-face with someone who may be able to resolve their complaint. This is not necessarily possible with electronic transactions, either because the merchant may not have a physical location or it may be some distance away.

A study undertaken by Consumer Affairs Victoria in May 2003 found that of Australian trader websites, only 4 percent had clear information about complaints handling procedures.[65] Further, just identifying that such procedures are in place does not necessarily mean that these procedures are transparent or fair.

In m-commerce transactions, the issues of how complaints will be dealt with and how these can be brought to the attention of the trader are complex. As noted above, given the limitations of the technology, it is not necessarily feasible for these processes to be clearly articulated to consumers. Furthermore, it is likely that new traders will enter the m-commerce market, without the appropriate complaints handling and dispute resolution procedures in place.

Industry approach to the issue

Telecommunications agencies currently involved in providing m-commerce services have not identified this as a potential issue for consumers. In general, there is an

[64] *ibid*.

[65] Minister for Consumer Affairs, 2003, *Victorian Consumers Face Problems Shopping Online*, Media Release, Tuesday, 11 March 2003. http://www.consumer.vic.gov.au

[66] ACA, 2003, *op cit*, p.6

assumption that where consumers have an issue with a product or with a contract, then it is up to the consumer to take up the matter with the message originator, just as he/she would if they had transacted via e-mail, telephone or online, and the message originator will be responsible for dealing with the problem. Where the goods or services being provided are dependant on the mobile phone service provider's network, they should take responsibility for the completion of this transaction.

The *BPM for Electronic Commerce* identifies the need for consumers to have access to mechanisms to resolve complaints and seek redress. It states that businesses should provide consumers with clear and easily accessible information about complaints handling procedures, endeavour to resolve any complaints and offer further advice on where to take a complaint should the issues not be resolved internally. ADMA also address this issue in its Code of Conduct for members, which states that consumers should have access to fair and timely alternative dispute resolution redress without undue cost or burden.

Neither of these documents provides any detail as to how dispute resolution processes should be established, particularly in the electronic medium.

Current regulatory protections in Australia

The TPA and state and territory legislation imply certain warranties into contracts for goods and services. These implied warranties include, in the case of goods, fitness for service, that services will be supplied with due care and skill. Implied warranties exist irrespective of whether suppliers also provide express warranties. Where implied warranties are breached, the consumer is entitled to redress, for example a refund or exchange.

At the Commonwealth and State and Territory levels there are a range of existing complaints handling mechanisms which may assist consumers with m-commerce related disputes. Existing alternative dispute resolution schemes include the Telecommunications Industry Ombudsman (TIO) and the Banking and Financial Services Ombudsman (BFSO). Regulatory agencies including consumer affairs agencies, the ACA and the Australian Broadcasting Authority also play a role in the resolution of consumer complaints. Finally, there are a number of low-cost small claims courts across the states which deal with civil disputes.

In submissions to the ACA consultation process on m-commerce, service providers expressed a view that existing dispute resolution services covering e-commerce and other commercial transactions would adequately deal with m-commerce transactions, and see no role for additional dispute resolution mechanisms to be put into place.[66] However, there could be scope to extend the role of the TIO to cover disputes over m-commerce.

International regulatory responses

There appears to have been no consideration given as to which party in an m-commerce transaction will be responsible or liable for a contested purchase. As noted above, the Korean Fair Trade Commission now requires the name of third-party content providers to appear on all telephone bills, enabling consumers who have a disputed transaction to follow up directly with the content provider rather than the telephone company. This implies that the actual delivery path by which an order is made will not affect liability for the transaction in Korea.

Recognising, however, that distance or non-contact transactions, that will include m-commerce transactions will inherently result in an increasing number of distance (or even cross-border) interactions and to disputes between parties located far from each other, the EU has put into place a number of additional protection mechanisms for consumers.

The 1997 *Distance Selling Directive*[67] addressed the issue of resolving consumer disputes across borders or long distances. The Directive requires Member States to ensure that adequate and effective means exist to ensure judicial redress for consumers. The 2000 E-Commerce Directive requires Member States to ensure that the legislation allows the effective use of out-of-court settlement schemes for dispute settlement, including appropriate electronic means. Article 17 of the Directive advises EU Member States to encourage bodies that are responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.

[66] ACA, 2003, *op cit*, p.6

[67] European Commission, 1007, *Directive 97/7 of the European Parliament and of the Council of20 May 1997 on the protection of consumers in respect of distance contracts* (O.J. L 144, 04/06/1997)

The European Commission[68] has conducted a significant amount of work in this area[69] that culminated in a proposal released in 1998. The proposal, contained in a European Commission Communication on the out-of-court settlement of consumer disputes (the "1998 Communication")[70], sought to improve consumers' access to justice through simple, swift, effective and inexpensive redress channels. In particular, it established:

- a complaint form, available in the 11 official languages of the EU, designed to facilitate communications between consumers and professionals and access to out-of-court procedures should an amicable solution prove impossible, and
- a recommendation on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes (the "Recommendation").

In order to overcome the obstacles for a consumer to access relevant out-of-court bodies in other Member States it has been necessary to create central contact points in each of those states. These will act as clearinghouses for providing information and advice to the consumer with a complaint about goods or services.

The Commission recently published a working document on the creation of a European Extra-Judicial Network (the "EEJ-Net")[71]. The EEJ-Net has the objective of acting as a one stop national contact point ("NCP") at national or European levels. At national level, it will provide local consumers with a single contact point where they can seek information about what out-of-court dispute resolution bodies exist in their jurisdiction and where they should address their complaint. At the European level, where the consumer has a complaint that arises from a transaction with a supplier located in another Member State, the NCP in the country of the consumer should be able to provide information and assistance. Such information would be obtained through the relevant NCP in the supplier's country. In addition the NCP would provide assistance to the consumer in formatting and filing his or her complaint and act as a national information resource for NCPs in other Member States who wish to advise their national consumers on the appropriate body in the jurisdiction to address their complaints. These tasks are not exhaustive and it is envisaged that once the EEJ-Net begins to evolve and develop, new functions and tasks may emerge.

The EEJ-Net will act as a primary point for the communication of complaints to out-of-court bodies. In this regard, it will:

- identify the appropriate body in its jurisdiction that can deal with a specific complaint
- provide advice about appropriate consumer dispute resolution schemes for particular complaints, and
- offer, through one NCP, the service of assisting consumers in the preparation of their complaints before transmitting it to another NCP.

The Commission has also established an EU-wide complaints network (FIN-NET) for consumers of cross-border financial services. Through this, consumer disputes are forwarded by consumer agencies (e.g. the Financial Ombudsman Service) to the relevant dispute resolution scheme in the service provider's country for resolution.

Key issues for consideration

- **Are current arrangements for the resolution of consumer complaints appropriate and adequate to deal with issues likely to arise from m-commerce?**
- **What options are available and suitable to hear and resolve consumer complaints in relation to m-commerce services?**

3.2 Financial issues

Financial issues are perhaps those that have been least rigorously tested in the context of identifying how the current regulatory frameworks will apply to m-commerce transactions. There are many types of electronic payments, including automated clearing house fund transfers, credit card payments and stored value or e-money payments.

[68] The European Commission manages and implements the policies of the European Union (EU).

[69] The urgent need for Community action in regard to the settlement of consumer disputes was highlighted and confirmed in the consultations on the Green Paper (1993) and the Action Plan (1996) on "consumer access to justice and the settlement of consumer disputes in the single market

[70] Stéphan Le Goueff, 2002, Resolution of Consumer disputes in the Digital World: *Desperately Looking for Confidence*, http://www.vocats.com

[71] See: http://europa.eu.int/comm/dg24/policy/developments/acce_just/index_en.html.

One of the challenges that e-commerce has faced over the last five years has been identifying a payment mechanism that can be used effectively in an online environment. The work that has been done on this front provides a basis for mobile payments. However, there are likely to be a number of consumer issues that will still require resolution, including security and liability issues. In addition, there may be a need to establish new processes to permit the use of mobile payments.

3.2.1 Protecting consumers from financial loss

Description of the problem

Protecting consumers from financial loss in m-commerce transactions encompasses protection from fraud resulting from either theft of bank or credit card details or failure to supply goods and services ordered and paid for. This section discusses failure to supply goods or services with card issues considered later in the paper as part of the discussion on security issues.

The need to protect and provide redress for consumers where merchants do not supply the good following the payment has been recognised as a key issue in the distance selling market.

Financial loss can also result from making purchasing decisions, perhaps as a result of pressure selling tactics or an inability to make an informed choice, due to failure to provide key information. In the electronic world, consumers will not have the opportunity to see and examine products before purchase. They are also unlikely to be able to obtain further advice from a merchant prior to making a purchase. Instead, the consumer will be relying on standard or generic information provided by the trader.

The Victorian Drugs and Crime Prevention Committee has recognised that Internet purchases are inherently more risky than offline purchases, based on the lack of physical presence in transactions, the capacity for deception and the speed in which online transactions take place, often denying parties an opportunity to "cool-off", verify evidence or identify the other contracting party. Like e-commerce transactions, m-commerce transactions carry similar inherent risks.

Industry approaches to the issue

In Australia, key protections for consumers making payments for a good prior to the goods being received have been developed through voluntary arrangements rather than statutory protections. Chargeback mechanisms allow consumers to charge the cost of the transaction back to the merchant. The merchant can dispute the claim, but ultimately the matter is decided between the card-issuing company and the merchant's bank.

The Australian Bankers Association (ABA) has addressed the issue of chargebacks in the recently revised *Code of Banking Practice*. All subscribers to the Code are required to provide general information on chargeback rights, the timeframe for disputing a transaction and a warning that the ability to dispute a transaction may be lost outside the applicable timeframe.

The Banking and Financial Services Ombudsman (BFSO) handles complaints relating to chargebacks and it is that body's general view that chargebacks are a consumer right. Where a bank fails to chargeback correctly, the consumer should be compensated for any loss without being required to attempt to recover against the merchant. While chargeback arrangements provide quite effective consumer protection, it is arguable whether consumers are aware of them or have any understanding of their operation.

The *Electronic Funds Transfer Code of Conduct*, developed under ASIC auspices, is a voluntary code which also provides consumers some protection in the case of unauthorised transactions where there is no contributory negligence on behalf of the consumer, for example disclosing a PIN to another party. Most, if not all banks are signatories to the Code. The BFSO has assessed the potential to use the EFT code for m-commerce transactions and has argued that it could be applied to m-commerce without amendment. Furthermore, under the new BFSO (previously the Banking Industry Ombudsman), non-bank financial service providers may now apply for BFSO membership. The TIO, in its assessment, has argued that the EFT Code could only apply to macro-payments involving the transfer of funds from a bank account or credit card. It is clear that some analysis will need to be undertaken to determine the extent to which the Code will apply.

The ADMA Code of Practice recognises the importance of consumer protections for electronic transactions. It identifies limitations of liability for unauthorised transactions or fraudulent use of payment systems and views chargeback mechanisms as tools that can enhance consumer confidence. It encourages members to use these mechanisms, but does not stipulate them as required by direct marketers who trade electronically.[72]

The Code stipulates that, when supplying goods or services at a distance, members must provide a seven day "cooling off" period during which a customer is entitled to cancel the contract with the direct marketer. In addition, members must ensure the customer's right to cancel the contract is specified in any contractual documents.

Key regulatory protections in Australia

Accepting payment without being able to supply, or supplying goods or services that are materially different from those agreed to, is a breach of both the TPA and state and territory fair trading legislation.

International regulatory responses

The Organisation for Economic Co-operation and Development (OECD) has identified a number of regulatory regimes protecting consumers against unauthorised use of cards, non-delivery of services and non-conforming goods and services.[73] The European Commission's *Communication on E-commerce and Financial Services* raises the possibility of a legislative safety net for consumers making payments online, similar to the chargeback system. The UK *Distance Selling Regulations* provide that if fraudulent use is made of a consumer's credit, debit or stored value card for distance selling, the consumer is entitled to cancel payment and be reimbursed in full by the card issuer. Under these regulations, the onus to show that a debit was authorised is placed on the card issuer.

In Canada, fair trading law requires a card issuer to cancel or reverse any credit card payment (and associated interest or charges) on request by the consumer if the consumer has exercised a cancellation right and the trader has not refunded within 30 days.

A recent announcement from the EU Commissioner for the Internal Market, Taxation and Customs Union foreshadows the plan to adopt a new EU directive enhancing consumer protection in electronic and credit card payments. A first draft, which is expected to be presented to the Commission in the coming months, includes a complete exclusion of cardholder liability for e-commerce transactions in which the cardholder does not receive merchandise or receives defective merchandise. In addition, cardholder liability for lost debit or credit cards shall be limited to 150 euros even if the cardholder has negligently contributed to the loss.[74]

Key issues for consideration

- **Is the self-regulatory framework that has been developed adequate to deal with increasing electronic trade, both online and using m-commerce?**
- **Should regulatory protections be considered to improve consumer protection in electronic payments and purchasing?**

3.2.2 Overcommitment to m-commerce services

Description of the problem

Within Australia most m-commerce currently involves the consumer paying for additional services on their phone bill; that is, the mobile service provider acts as an intermediary. With m-commerce services, consumers have the ability to run up a larger bill quicker than ever before.

The question of how to protect younger consumers who have access to m-commerce is also an issue of concern. A recent report commissioned by the NSW Office of Fair Trading, Youth Debt,[75] found that for young people debt is a serious issue, and one that is becoming a major problem. Bills associated with mobile phone use topped the list of troublesome bills for young people, with almost 50 per cent of the young people interviewed who were under the age of 18 placing it as the major contributor to their debt problems.[76] The capacity to conduct increasingly complex transactions and make payments using a mobile phone could lead to higher levels of mobile phone related debt,

[72] ADMA, 2001, Direct Marketing Code of Practice, http://www.adma.com.au, November 2001, p.10

[73] OECD Directorate for Science, Technology and Industry, 2003, *Report on Consumer Protections for Payment Cardholders*, Committee on Consumer Policy, 14 June 2002

[74] EUPOlitix.com, 2003, *Banks to foot consumer protection bill*, http://www.eupolitix.com/EN/News/ff7df681-b4e4-4471-b70f-6e79bff8c923.htm

[75] NSW Office of Fair Trading, 2003, *Youth Debt: A Research Report*, prepared for NSW Office of Fair Trading by Daugar Research. November 2003. p 18

[76] *ibid*.

in particular if there are no protection mechanisms put into place to prevent large bills being accrued without the user necessarily being aware.

A related issue that has been brought to the attention of fair trading agencies has been the use of 190 premium telecommunication services to make purchases. Consumers may tally up large phone bills as an unintended consequence of making a purchase. As an illustration, in one case recently considered by Consumer Affairs Victoria, a person aged under 13 racked up over $300 in call charges for purchasing and downloading mobile phone ring-tones via a 1902 number service.

As m-commerce grows, it is expected that consumers will be able to transact directly with content service providers. Credit card transactions may take place entirely via SMS, WAP or on wireless-enabled websites. Mobile carriage service providers may not always contact the customer when a credit limit is exceeded.

Industry approaches to the issue

Current technologies and processes provide mechanisms to control credit limits or spending authorisations, irrespective of how the payment is made. Industry states it is primarily the consumer's responsibility to monitor their expenditure on phone calls, including premium rate services.

Nevertheless, there are some protections that have been brought in by industry to protect risk and improve consumer's overall credit management in relation to telecommunications services.

In response to the increasing problems of customer debt, the Australian Communications Industry Forum (ACIF) has developed a code of conduct, enforceable by the ACA. The *Credit Management Code* covers the provision of credit in the supply of telecommunications services and regulates the supplier's activities in seeking payment for services provided.[77] It sets minimum standards of practice that suppliers must adhere to in assessing the credit of customers and defines the procedures suppliers must follow for the restriction, suspension and disconnection of a customer's service. Under the Code, customers can limit access to a supplier's service and impose a limit on their expenditure for any service. Suppliers can also impose restrictions on the supply of services for customers, providing information as to how and why decisions have been made are given to consumers. Suppliers must also provide customers with options to manage bills, including flexible payment options. The Code also clarifies the use of guarantors by industry and requires suppliers to advise the guarantor of their level of risk. A focus of the Code is on the debt-recovery practices of the suppliers.

The TIO will accept complaints about breaches of the *Credit Management Code*, which gives consumers some additional redress if they are unable to resolve the issues with the service provider. The TIO has identified complaints in relation to credit management as a difficult area, with nearly 2,400 credit-related complaints from residential and small business consumers in the three months from June to September 2003. A large proportion of these were related to the debt collection practices of suppliers and other agents who have purchased debts or are collecting debts on behalf of suppliers.[78] The extension of the *Credit Management Code* to cover m-commerce services is likely to assist in dealing with consumer concerns about unexpected bills and problems in paying such bills but the issue remains of who bears the responsibility to protect consumers – the carriage service provider or the content provider. Are carriage service providers merely the billing agent on behalf of content providers or are they responsible for managing the risk for customers and content providers?

It has been argued that industry has already sought to address problems of unexpectedly large bills through the introduction of a Code of Practice. Under the Telephone Information Services Standards Council (TISSC) Code of Practice, all 190 services have call cost warnings and can only proceed after a positive consumer acknowledgment. Additional price warnings are broadcast throughout the call.

However, ADMA has expressed some concerns about the capacity of TISSC to respond to problematic industry practices in regulating premium services. It claims that TISSC is a "toothless tiger" only able to make recommendations to the carriers for action and that there have been countless occasions where the carriers have not implemented the recommendation.[79]

---

[77] Australian Communications Industry Forum (ACIF) 2003, *Industry Code – Credit Management*, ACIF April 2003

[78] Telecommunications Industry Ombudsman (TIO), 2003, *Telco credit management practices remain a cause for concern*, TIO Media Release, Thursday 9th October 2003

[79] Australian Direct Marketing Association (ADMA), 2003, *Discussion paper regarding the need for additional regulatory measures in relation to the supply of premium services*, Submission to the ACA inquiry, http://www.aca.gov.au/aca_home/issues_for_comment/discussion/comments.htm accessed 13 September 2003

With the increasing uptake of SMS and MMS, Telstra has already sought to address potential problems of large bills. It has been reported by the Small Enterprise Telecommunications Centre (SETEL) that Telstra will send a notification to a consumer when a $200 limit is reached. This approach, however, seems to have been based on the carriage service provider's own risk management strategies for managing the problem of high bills that a consumer cannot afford. It has been argued that this approach will be ineffective based on concerns with difficulties in assessing real time usage and possible delays in sending warnings.

It can be expected that service providers and carriage service providers will adopt traditional methods to disseminate information to customers about the potential problem of unforeseen bills, including websites, telephone bill inserts and SMS warnings.

Current regulatory protections in Australia

Credit management of telecommunications products and services is not currently subject to an over-arching regulatory regime. There are some legislative requirements covering credit management practices under the *Privacy Act* 1988, but these legislative requirements are not consolidated in one package that can be easily accessed by consumers.

The issue of protecting consumers from unexpectedly high bills and the potential for this to occur with the new premium rate messaging services is being explored by the ACA. The ACA has prepared a draft *Telecommunications Service Provider (Premium Services) Determination 2003*. Under the proposed determination, if a relevant customer incurs charges of $250 in a month for 190 premium services, the relevant 190 carriage service provider must bar all future calls by the customer to all 190 premium services for the remainder of that month, unless the application of this subsection has been waived.

However, this approach will not deal with the issue of high bills that are generated through purchases of other products using m-commerce. The issue will be further complicated by the introduction of the content provider and, potentially, the finance provider, into the relationship.

International regulatory responses

The issues of managing credit and debt and the financial overcommitment to electronic services have not been identified as an area where any specific regulatory action has been taken internationally.

Key issues for consideration

- **What protections should consumers have, especially when unexpectedly high bills are becoming commonplace in this industry?**
- **Is it the consumer's responsibility to manage their limit?**
- **What practical steps could be put into place to reduce the problem of unexpectedly large bills?**

Is there protection under legislation?

Australia's credit laws

The Consumer Credit Code applies to consumer lending that is primarily for personal, domestic and household purposes. The Code has a number of protections for consumers, including:

- disclosure of the amount of credit, or maximum amount of credit agreed by the parties, and
- a statement of all fees and charges that are, or may become payable must be provided to consumers in the contract.

The Code also gives consumers certain rights and protections if they get into financial difficulties and fall behind in their loan repayments as well as protections in respect of enforcement.

The Australian Capital Territory (ACT) has made a recent amendment to its *Fair Trading Act* to require credit providers to undertake a "satisfactory assessment process" of a debtor's credit-worthiness before a credit card limit is issued or a increase is approved[80]. A satisfactory assessment process, in relation to a debtor, is an assessment of the debtor's financial situation sufficient to satisfy a diligent and prudent credit provider that the debtor has a reasonable ability to repay the amount of credit provided or to be provided.

[80] ACT, 2003, Fair Trading Act 1992 (section 28A), http://www.legislation.act.gov.au/a/1992-72/default.asp

Will these apply to m-commerce?

The Code would certainly apply to credit linked to m-commerce that simply involves the consumer using an existing credit card to purchase goods over the phone There is a growing concern that one of the most likely m-commerce payment models will effectively offer people another type of "credit", whereby payment for goods and services purchased is deferred until the telephone bill arrives. This has gained increasing attention with the launch of the "Dial a Coke" trial by the Telstra Corporation and "Coca Cola", whereby people can order and pay for a drink that they receive instantly, but pay for it later.

The debate that has emerged is whether these services could or should be regulated under existing credit laws – in particular using the Consumer Credit Code. However, the definition of credit under the Credit Code makes this problematic. To be considered as a credit contract, a number of preconditions must be met.

One of these preconditions is that the Code only applies if a charge is or may be made for providing the credit. At present, there are no examples of a telephone service provider that charges an additional fee, either per transaction or as a regular fee, for m-commerce payment facilities. The Code also does not apply to credit limited to a total period of 62 days or less, unless the credit is a high-interest loan. A majority of mobile phone bills are settled within this period and the debt on a mobile phone typically becomes due in full at the time of each bill.

It appears that current telco-billed m-commerce services would not be considered as regulated credit. However, the Code clearly could apply as the market develops new mobile payment services that may fall within the Code's application. The issue is whether existing telco-billed m-commerce services are similar enough to credit to warrant additional consumer protections, and, if so, how those protections should be introduced.

3.2.3 Billing and charging to a mobile

Description of the problem

The ability to make payments using a phone and have these added to a monthly account raises additional issues for consumers in terms of billing and charging. How transactions are charged to accounts and the information that is provided to consumers in terms of the bills are likely to be key to consumers keeping track of their transactions and payments. The issue also raises concerns about the consumer's ability to dispute charges.

Industry approaches to the issue

ACIF has recognised the need for billing accuracy for telecommunications services. It has developed a Code that specifies the requirements for checking the accuracy of call charging and billing of fixed line and mobile telephone services in Australia that provide voice-telephony. All carriage service providers must adhere to the Code, which is overseen by the ACA. The Code primarily addresses the testing regime required to ensure accurate billing, sets minimum performance targets in relation to overall accuracy of the billing system and identifies standards for billing accuracy. While the Code establishes a requirement for accurate billing for services, it does not cover issues associated with customer billing and is limited only to the provision of standard voice services, which effectively excludes an application to billing for m-commerce services.

A revised Billing Code was developed in February 2003[81] that sets minimum standards for suppliers to ensure that customers receive acceptable levels of service, including: bill content, itemisation and verification of accounts, options for payment, direct debiting and access to information about a bill. The Code covers carriage service providers and content providers, including pay TV operators. Compliance with the Code has obliged existing suppliers to modify their billing policies and associated procedures, including staff education and training, to ensure broad awareness of the required functionality.

The Billing Code is not limited to the provision of voice telephony and, given its application to content service providers, will extend to the ways in which m-commerce services are itemised on mobile phone accounts. This will be an important mechanism to enable consumers to read and understand their bills and their expenditure on m-commerce services. Under the Code, the TIO has the power to handle end user complaints, including facilitating the resolution of, and making determinations in relation to matters arising under the Code.[82]

[81] Australian Communications Industry Forum, 2003, *Billing: Industry Code*, February 2003

[82] *ibid*. p.33

Current regulatory protections in Australia

The ACA can enforce the Billing Code under the *Telecommunications Act* 1997. However, other than this mechanism, there are very few protections that exist for consumers in relation to billing for standard purchases.

The Consumer Credit Code provides some consumer protections in relation to the sort of information that is to be provided to consumers who are in a credit relationship with a financial service provider. The Code, which commenced operation on 1 November 1996, governs credit given wholly or predominantly for non-business purposes. The Code applies only if a charge is or could be made for providing the credit.

Under the Code, there are a number of disclosure requirements for credit contracts. Credit providers must disclose: details of the credit fees and charges that are, or may become, payable under the contract, when each fee is payable; and the amount of any credit fee or charge and the total amount of credit fees and charges. The Code also requires the credit provider to disclose: any commissions paid by or to the credit provider; and whether any of the financial conditions, such as the interest rates, can be changed and how consumers will be notified of these changes.

Of note, the Uniform Consumer Credit Code Management Committee (UCCCMC) is currently working towards amending the Consumer Credit Code with the aim of implementing the e-commerce recommendations made in the Post Implementation Review (PIR) of the Code. The PIR review recommended that electronic transactions should be recognised by harmonising the Code, as far as possible, with the Electronic Transactions Bill 1999. In addition, it was recognised that the Code would need to adopt specific consumer protection measures to respond to issues that arise out of the consumer credit environment.[83]

However, bills for telecommunications services, including the monthly mobile phone account, are unlikely to be considered as credit under the Code and, therefore, the protections that exist for consumers in credit contracts will potentially not exist for other payment mechanisms.

International regulatory responses

Some state legislatures in the United States have adopted additional protection mechanisms that support m-commerce. From 1 July 2001, the Californian Public Utilities Commission has regulated the use of mobile telephones as payment devices when the charge is billed to the consumer by the wireless telephone service provider.

The intent of the law is to protect consumers and businesses against abusive billing practices. 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 and agents and vendors using billing services. 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.[84]

Key issues for consideration

- **Are current approaches to billing adequate?**
- **Are additional consumer protection measures required and, if so, what form should these take?**

3.2.4 Protecting funds on a mobile phone

Description of the problem

The concept of the e-wallet, where the mobile phone stores electronic money (e-money) that can be accessed to make payments, is one that has been widely discussed since the developments of the first smart-cards, but has yet to emerge as a payment mechanism for electronic transactions.

The EU has defined e-money as monetary value stored on a chip card (pre-paid card or 'electronic purse') or on a computer memory (network or software money) and which is accepted as a means of payment by undertakings other than the issuer.

[83] Clyde, I. 2003, *Click Here for Details: E-commerce and Consumer Credit*, Paper prepared for the Uniform Consumer Credit Code Management Committee, September 2003. p.1

[84] Caldwell, K. 2001, Federal Government and States to Regulate Mobile Payments, *The Public Policy Report, CommerceNet Newsletter*, Vol 3, No. 7, July 2001, http://www.commerce.net

Such schemes are likely to be popular among consumers who do not own credit cards and lack the capacity to make and pay for instant purchases electronically. The e-money is usually loaded onto the phone's SIM card via a direct debit from a credit or bank account and can then be used to complete transactions.

Along with the relative ease of such transactions come a number of problems. Most importantly, there is unlikely to be any banking approval process to access the funds and the security of the funds will be closely linked to the handset and the security features that are activated by consumers.

Industry approaches to the issue

As noted earlier, the *Electronic Funds Transfer Code of Conduct* will provide consumers with some protection in the case of unauthorised transactions where there is no contributory negligence by the consumer, such as, disclosing a PIN number to someone.

However, mobile phones are easily stolen and loading them with funds leaves consumers vulnerable to unauthorised transactions. In situations where a mobile phone is stolen and the funds on a mobile are accessed, the extent to which this Code will apply is arguable.

Current regulatory protections in Australia

No legislative protections that would cover consumer liability in the event of a mobile phone being stolen or purchases made without consent have been identified as part of this study. It has been largely left up to industry to develop alternate approaches to responding to these problems.

International regulatory responses

In 2002, the UK Treasury, acting on a European e-money directive, made e-money a regulated activity under the *Financial Services and Markets Act* 2000. Mobile carriage service providers issuing e-money on mobile phones must be authorised, supervised, have certain resources and maintain certain levels of capital, provide certain information to consumers, limit electronic purse values to a certain maximum value and maintain a complaints policy.

Key protections include:

- limiting the purse size: The risks associated with the use of e-money warrant a limit of £1000 per purse. A higher purse limit may be permitted where certain safeguards are met, and
- prescribing the conditions for discounted e-money: E-money issuers are allowed to issue e-money at a discount for marketing purposes in certain tightly controlled circumstances.

However, issuers of e-money are not subject to the same regime as credit institutions and the UK's Financial Services Compensation Scheme[85] does not apply to e-money issuers. As a consequence, consumers have no access to compensation should an e-money issuer become insolvent. E-money issuers are, however, included within the scope of the Financial Ombudsman Service and must also have their own procedures for dealing with customer complaints.

In Korea, there has been concern with the use of e-money. Korea's Financial Supervisory Service stopped mobile carriage service provider SK Telecom from making chips that made mobile handsets equivalent to credit cards. An official said there would be confusion if non-financial companies had access to individuals' credit card information[86].

Key issues for consideration

If e-wallets are not considered credit cards, should they be regarded as cash or do consumers need some middle-of-the-road protections?

3.3 Privacy

Privacy issues have been a key reason for potential online consumers to avoid e-commerce. 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 unauthorised access to stored data, especially personal information and transaction history.

[85] A safety net for customers of authorised financial services firms, created under the *Financial Services and Markets Act*, 2000

[86] Korea Times, Jan 2003

3.3.1 Wireless spam

Description of the problem

Spam is unsolicited bulk messaging, and has been recognised as the scourge of online communication. SMS and other wireless spam is now already on the increase as mobile phones become a favoured medium for marketing. The following graph illustrates the explosive growth in SMS advertising across the globe, and, based on current trends overseas, both SMS advertising and unwanted SMS spam in Australia is expected to increase.

Figure 3: Advertising messages delivered to mobile phones – customer's experiences[87]

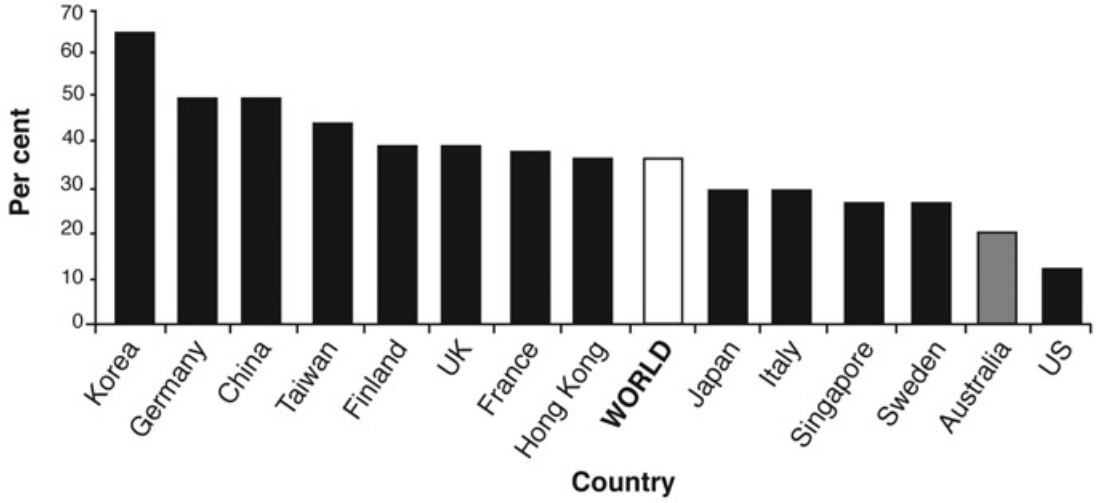
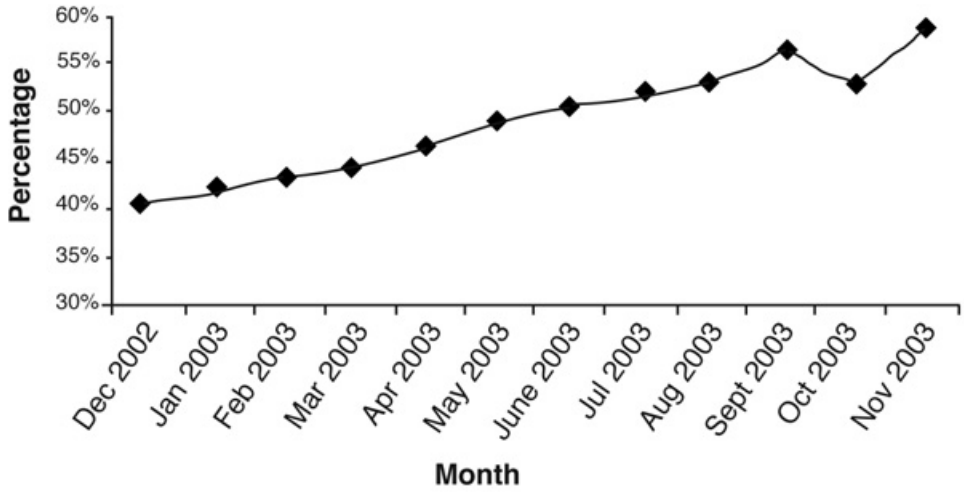


Figure 4: Growth in spam, Percentages of total Internet email identified as spam (international estimates)[88]



[87] AT Kearney, 2002, *op cit*.

[88] Brightmail, 2003, *Spam Statistics: Spam Percentages*, www.brightmail.com/spamstats.html. Accessed 12 December 2003

One issue is the ability for consumers to complain about or object to spam. Some SMS service providers also make it harder than necessary to unsubscribe from messaging, burying the process deep within a website.

Industry approaches to the issue

Industry participants generally agree that carriage service providers have some responsibility to ensure that their advertisers are aware of the correct manner of communicating with consumers. However, they do not accept responsibility for the content of advertisements.

In 2002, ACIF recognised the potential to use SMS for marketing and advertising and introduced a Code to guide carriage service providers and service providers in using SMS for the delivery of marketing messages to mobile telephone customers.[89] The SMS Code reflects a recognition that SMS technology can be very intrusive, if abused. It aims to reduce the incidence of unsolicited marketing messages received by customers and, unlike the ADMA Code, places the onus of protection on carriage service providers and mobile service providers.

Under the Code, carriage service providers must ensure that all marketing messages include a "Recognised Identifier" to enable a recipient to directly contact the organisation that sent the message. Carriage service providers must also make sure that there is a process recipients can use to opt out of receiving SMS messages. There is an exemption for the sending of SMS messages that relate to health, safety and law enforcement matters and service-related messages. Complaints can be handled by the TIO.

However, the Code does not deal with SMS message originators that do not have a commercial arrangement with a carriage service provider for the transmission of an SMS message. Also, the Code does not deal with end users sending SMS messages from their mobile phones. In this sense, the effectiveness of the Code is limited. It may also not be applicable to the use of location-based marketing, which is discussed further below. The Code has been registered by the ACA, meaning it can be enforced legally.

The ADMA *Code of Marketing Practice* includes some specific provisions regarding marketing using email and SMS that aim to reduce the invasiveness of marketing via mobile phones. In addition, ADMA's Mobile Marketing Council has developed a *Code of Practice for Mobile Marketing* which sets out the standards that must be achieved by all ADMA members when marketing or offering products and services via mobile technology. Members must not send random unsolicited, untargeted messages and must only send messages to people who have consented to receive such messages or to customers with whom members already have a relationship.[90] However, there are a number of concerns with the content of the Code from a consumer protection point of view. A key issue is its lack of detail, particularly about issues such as marketing to children. According to the Code, a member must not deliberately target children with premium rate services, but there is no detail about the age bracket for children, and there is some concern that marketers are still able to send messages that contravene the spirit if not the letter of the Code.

Message originators sending commercial communications must operate and maintain an in-house suppression file, listing recipients who have indicated that they do not wish to receive further communications. Details of the customer must be removed from the database within 14 days of the request. The Council has also developed a national Mobile-Marketing Opt-out Service for consumers who do not wish to receive any mobile marketing messages.

Current regulatory protections in Australia

In addition to the array of self regulatory codes that cover marketing and advertising practices, the use of personal information is also covered by privacy legislation. The Privacy Act 1988, and the amendment introduced in 2000 that extends coverage of the Act to the private sector,[91] includes the National Privacy Principles (NPP).

In the private sector, the NPPs cover aspects of the use, collection, storage and disclosure of personal information. Messages sent by carriage service providers to their customers are covered by the provisions of privacy legislation and the Privacy Commissioner's Guidelines to the NPPs consider the use of SMS for marketing. Under the requirements of the Privacy Act, prior consent must be obtained for the use of personal information for marketing activities unless the marketing would be within the

[89] Australian Communications Industry Forum (ACIF), 2002, *Short Message Service (SMS) Issues, Industry Code ACIF C580:2002.*, August 2002

[90] ADMA, 2003, M-Marketing Code of Practice, http://www.adma.com.au, June 2003

[91] Privacy Amendment (Private Sector) Act 2000, Commonwealth Government

reasonable expectations of the individual or is for direct marketing purposes subject to certain conditions.

While the use of personal information to market to individuals is covered by privacy legislation, the reference in the *Privacy Act* to direct marketing does not deal specifically with SMS messages and does not cover some small businesses, which may include many message originators. There is reference to the use of SMS for marketing in the Privacy Commissioner's Guidelines to the National Privacy Principles, but only in relation to whether prior consent has been obtained. In addition, these guidelines are not legally binding.

On 2 December 2003, the Australian Government passed the new anti-spam legislation which includes:

- a ban on the sending of commercial electronic messaging without the prior consent of end-users unless there is an existing customer-business relationship (an opt-in regime)
- a ban on the distribution and use of e-mail harvesting or list-generating software, and
- civil sanctions for unlawful conduct including financial penalties, an infringement notice scheme and the ability to seek enforceable undertakings and injunctions,
- the requirement for all commercial electronic messaging to contain accurate details of the sender's name and physical addresses and a functional 'unsubscribe' facility to enable people to opt-out, and
- a commitment to work with international organisations to develop global guidelines and cooperative mechanisms to combat the global spam problem.

The Government has stated that it will work with industry to ensure that Australia has a workable regime without harming legitimate business practices. There will be a 120-day sunrise period without penalties from the enactment of the legislation to enable businesses to ensure that their marketing practices are in line with the legislation.

The ACA will be responsible for enforcing the new legislation and has begun setting up a dedicated unit to enforce the new anti-spam law. The unit would be working with industry to develop appropriate codes for registration, and to investigate spamming and ensure compliance.[92]

The extent to which these anti-spam laws will apply to mobile marketing has not been addressed by the Commonwealth in the announcement of its intention to regulate in this area, however it is assumed that these laws will also apply to spam messages sent via mobile phones.

International regulatory responses

The EU's Directive 2002/58/EC[93], which came into force on 12 July 2002, explicitly aims to deal with privacy issues associated with mobile electronic communications. Under this Directive, the sending of marketing e-mails or SMS messages requires prior explicit consent. When gathering an electronic address for marketing purposes the consumer must be told about their use for direct marketing. Where there is an existing relationship, a company may only use the electronic address for similar products or services and it must be the same company. A consumer must have details about opting out of direct marketing within each message. False identifiers, return numbers or addresses are prohibited.

In general, the EU has strongly focused on the protection of individual and societal rights, particularly with respect to personal and data privacy. In May 2002, the European Parliament agreed with the position taken by the Council of the Union that unsolicited commercial communications sent by e-mail or SMS are not allowed without the prior permission of the user.

The UK's new *Communications Bill* contains several passages relating to mobile content and the use of mobile phones. The proposals would ban unsolicited text messages. The Advertising Standards Authority also updated its code of practice in March 2003 to cover advertisements sent to mobile phones.

In the United States, the CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act came into effect on 1st January 2004. It comprises an opt-out regime and legalises certain forms of spam. Unsolicited messages must contain a facility to opt-out of further communications, must not contain false headers and must be labelled as an advertisement.

[92] ACA, 2003, ACA welcomes anti-spam bill, Media release no. 57, 2 December 2003

[93] European Commission, 2002, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*

The H.R.71 *Wireless Privacy Protection Act* of 2003, if passed, would require customer consent to the provision of wireless call location information.

During 2001, the Wireless Advertising Association (WAA) – previously known as the Mobile Marketing Association (MMA) – 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/MMA also declared that wireless unsolicited advertising spam would serve the needs neither of consumers nor of the wireless industry and that the 'Confirmed Opt-in' should become the de facto standard for wireless push advertising (MMA, 2002).

Key issues for consideration

- **How does the consumer actually opt-in or out on phones as they are today? Will this have to be done at the time of the service contract?**
- **What additional protections need to be put into place to protect consumers from receiving unsolicited commercial advertising on their phones?**

3.3.2 Collection of location information

Description of the problem

A typical mobile phone sends out signals approximately every ten minutes that identifies the location of the nearest mobile phone tower. In less populated areas, these towers may be located every 20 to 50 kms; however, in major towns and cities, they can be as close together as 500 metres to 1 km. These signals can be used to determine a phone user's location. While this information is not being used at the moment, new business models will enable service providers and carriage service providers to archive and use such information to offer advanced locational services.

It is predicted that advertisers will offer discounted or free services in exchange for consumers accepting advertising and locational services. Many consumers are also likely to be willing to pay for certain applications and the customised delivery of information. This means that detailed personal information could be collated and tracked whenever a customer's mobile device is on, constituting a potential threat to both privacy and physical safety.

The provision of effective notice about information practices will be challenging in a practical sense because the screens on most wireless devices are so small that privacy policies will be difficult to read.

Industry approaches to the issue

Industry bodies consulted as part of this study agree that the issue of collecting and using personal information for the purposes of marketing and targeting services for m-commerce is one that should be addressed through industry codes and general statements of ethical behaviours. There is an implied assumption that carriage service providers will not be offering services or use m-commerce to market products or services to consumers who do not explicitly opt-in to receive such information. The ADMA *Mobile Marketing Code* states that location-based services and commercial communications must only be sent to recipients that have provided express consent to the receipt of such communications, at that time, from the message originator.

Current regulatory protections in Australia

The issue of using personal information collected from a mobile phone for direct marketing or other purposes is limited by existing privacy legislation in Australia. The private sector amendments to the *Privacy Act*, passed in 2001 state that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. It also states that an organisation must only collect personal information by lawful and non-intrusive means.

The *Telecommunications Act* 1997 (Cth) also contains a number of provisions dealing with the privacy of personal information held by carriage service providers, carriage service providers and others. Part 6 provides for the development of industry codes and standards in a range of consumer protection and privacy areas. The Federal Privacy Commissioner has the role under the Act of monitoring compliance with the privacy provisions.

It is likely that due to the sensitive nature of this issue, that carriage service providers and other industry stakeholders will be encouraged to develop industry-based approaches to protecting the information of their customers and restricting the use of this information without customer consent.

International regulatory responses

EU member countries are currently examining the privacy issues associated with processing data, including the use of mobile devices to obtain locational information. The 15 Members have agreed on the need to protect individuals by imposing the principle of 'prior consent by subscribers'

before any use is made of location data. Subscribers should have the means to temporarily suspend the processing of location data, even if they have consented to a location-based service (initially the proposal was to require a subscriber has given explicit consent to being locatable).

Users must also be able to express their refusal to have their movements tracked by their carriage service provider. Issues relating to how long personal data can be kept are also under debate, with proponents of limiting this time period in order to comply with a 'right to oblivion' (erasure of data) coming up against judicial authorities wishing to preserve personal data to facilitate any possible future litigation.

Korea's Ministry of Information and Communication is pushing ahead with a revised law that would make it obligatory for mobile handset makers to embed location-based service functionality in their consumer products[94]. However, this is presumed to be more from the perspective of responding to an emergency than enabling locational-based advertising to mobile phones.

In the United States, the *Wireless Communications and Public Safety Act* of 1999 amended the Telecommunications Act with a provision requiring carriage service providers to obtain express authorisation before releasing locational information to third parties. The information collected about a customer's location is also to be treated as customer proprietary network information, which receives special legal protections under the *Telecommunications Act*.

Key issues for consideration

- **How does Australian privacy legislation protect wireless information exchange?**
- **Are additional safeguards required for the use and collection of locational information from m-commerce. Will there be restrictions on companies who can collect locational information about consumers from their mobile phones?**
- **Can a privacy policy be displayed on a mobile phone?**

3.3.3 Retaining records of personal data

Description of the problem

Consumer concern about the privacy and security of personal information has emerged as a major barrier to participation in electronic commerce, as has concern about the proliferation of databases of personal information.

At present, carriage service providers may not be collecting and keeping much personal information about individuals through tracking and monitoring of mobile phone transactions. However, with the additional capability m-commerce offers to record and track electronic transactions, not to mention where these transactions take place, it is likely that customer profiling will increase rapidly.

The existence of a relatively small number of large collections of personal information represents just one of the challenges posed by customer profiling. There are now a very large number of small and medium sized collections of personal information. Indeed, many Internet companies have had business models explicitly built upon the collection, use and disclosure of personal information.

With increasing convergence and partnerships between industry sectors in the delivery of m-commerce services, the potential to share personal information is of further concern. Data collected offline (say through customer billing records) that is used to personalise or customise wireless advertisements could bypass some consent provisions. It has been foreshadowed that businesses will seek to collect large amounts of highly personal information for use in customisation. This will also provide opportunities for abuse by the companies collecting it and inevitably compromise the anonymity of making a purchase.

Industry approaches to the issue

Discussions with industry organisations highlight the threat to privacy that m-commerce potentially poses, in particular with the capacity to track and retain personal information for commercial purposes, or even on-selling the data.

It has been suggested that carriage service providers can make privacy disclosures in the initial service contracts for wireless devices. However, many content providers may not require consumers to sign service contracts before providing services.

An interesting development has been the recent release of the Internet Industry Association (IIA) Cybercrime Code of Practice. In an attempt to reduce the incidence and impacts of crime activities conducted over the Internet, the Code would require customer information collected by ISPs to be retained for six or 12 months, depending on the type

[94] http://www.koreaherald.co.kr/SITE/data/html_dir/2003/03/25/200303250011.asp

of information. Personal information, such as a customer's name, username, email address, phone number, credit card details and address must be retained for six months from the date a consumer ceases to be a customer of the ISP.[95]

In drafting the Code it was recognised that there may be some privacy concerns with the requirements to retain data. However, it was determined that there needs to be a balance between retaining records for security purposes and protecting the privacy of individuals, and that there are already regulatory protections in place to protect the privacy of individuals in the Privacy Act and the *Telecommunications Act*, as discussed below.

Current regulatory protections in Australia

The Commonwealth *Privacy Act* 1988 and the *Privacy Amendment (Private Sector) Act* 2000, as well as setting out how organisations should collect, use, disclose, keep secure and provide access to personal information, give individuals the right to know what information an organisation holds about them and a right to correct that information. The Act sets a standard that applies to all information, regardless of whether it is kept in the physical world or the virtual world.

Individual organisations are encouraged to implement the NPPs through the development of codes of conduct, which can be approved by the Privacy Commissioner. Given the breadth of the NPPs, these codes are intended to identify specific measures that organisations will undertake to ensure the protection of an individual's personal information. However, there has only been a limited response to this process to date.

The limitations of the privacy legislation lie in the application of the Act. Currently, small businesses do not have to comply with the Act.

The *Telecommunications Act* makes it an offence for service providers to disclose customer information to anyone other than law enforcement agencies and obliges carriage service providers and carriage service providers to make records of all disclosures of personal information (with only a few exceptions). It also requires disclosure to law enforcement agencies only in specified circumstances. The Federal Privacy Commissioner has the role of monitoring compliance with this part of the Act.

As m-commerce grows and, with it, the demand for personalised and customised services, providers can be expected to collect, and store increasing amounts of personal information in order to stimulate uptake and fulfil orders, conduct marketing programs and even generate profits from its sale. Retaining data electronically will make it even easier to collect, analyse and use information about individuals. The use of locational services will provide a further level of detail to personal information, such as shopping and recreational habits, etc.

Furthermore, the level of consumer awareness of the requirements of organisations to comply with the legislation may not be extremely high. Small handsets will limit the extent to which providers can adequately publicise their privacy policies.

International regulatory responses

The EU's E-commerce Directive outlines the importance of data protection in relation to E-commerce and makes direct reference to the European Data Protection Directives 95/46/EC and 97/66/EC. Vendors and buyers must be aware that any e-commerce transaction is potentially subject to data protection issues.

Some EU countries are requiring or allowing service providers to retain data when not strictly needed in case of a criminal investigation. However European data protection law only allows service providers to retain personal data for billing purposes and delete it afterwards.

Key issues for consideration

- **Are there sufficient protections for customer personal data and information?**
- **Are current protections sufficient to deal with the collection, storage and use of location-based information?**

3.4 Security

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

[95] Levinson, E. & Ceola, N. 2003, Cybercrime Code of Practice for ISPs, *Internet Law Bulletin*, Vol 6, No. 5 2003. p.57

3.4.1 Confidentiality and integrity of data

Description of the problem

A key difference between m-commerce systems and other electronic systems over which transactions are handled is the identification of the customer and the merchant. In a mobile payment system, the identification is the mobile phone number. Wireless devices are easy to misplace and relatively easy to steal. As mobile phones become capable of storing more information and conducting more sophisticated information processing, consumers will have more information at stake if they lose their devices. This raises obvious questions for a merchant, in terms of how they authenticate the user, and for the consumer, who could be liable for unauthorised transactions if their phone is used without their permission.

It is generally agreed that strong authentication procedures need to be in place to prevent security breaches. These need to be intuitive and transparent to users.

The issue could be compounded by problems with the delivery of m-commerce messages. SMS is a store-and-deliver system with no guarantee whatsoever that the message will get through. There are questions over the reliability of SMS. A January 2003 Keynote Systems study in the US found that 7.5 per cent of SMS messages are somehow lost.[96] This raises the associated issue that consumers are being charged for SMS messages that do not reach their targets, and they may not be even aware of this problem.

Network limitations could further compound authentication problems. Initial reports about Hutchison's new Australian 3G service have been somewhat disappointing. Early subscribers have complained about frequent dropouts, faulty handsets, poor battery life, unresponsive customer support and blackspots.[97]

Industry approaches to the issue

Currently, many mobile phones are enabled with locks to prevent unauthorised access to them. Advances in technology could allow the owner to lock the device from a remote location if it is lost. Other approaches being considered by equipment manufacturers include enabling users to load and unload their own privacy and security technologies and separating personal identifiers from transactional data. Wireless security could also be improved by implementing stronger authentication functions using public key infrastructure. In Europe, one standards working group is developing a small graphic that could be displayed on a phone to show that the transaction is secure.[98]

Using secure technology, such as that provided by smart-cards and secure payment gateways, is the only way to maintain protection against financial risk and cover merchants and consumers against fraudulent transactions. The development of biometric security features on handsets and wireless digital certification will also give consumers more confidence in wireless banking.

In June 2003, Japan's NTT DoCoMo said it would introduce SSL (Secure Socket Layer) security on its 3G service FOMA (Freedom Of Mobile Multimedia Access). A digital certificate is stored in a removable card in the handset and identifies the user to a mobile Internet trader.

Current regulatory protections in Australia

The current Commonwealth legislation relating to electronic signatures is the Electronic Transactions Act 1999 (which allows an electronic signature in place of a written one where required under a law of the Commonwealth).

The ETA also stipulates a uniform method for attributing the time and place of dispatch and receipt of electronic communications. This can be important in many transactions. Generally, a contract is taken to have been formed at the place where acceptance of the offer to transact is received. The ETA provides that receipt of an electronic communication occurs at the *place of business* of the addressee or, if the addressee does not have a physical place of business, at the addressee's ordinary place of residence. The time of receipt is the time when the electronic communication *enters an information system* designated by the addressee. If no such system has been designated, then an electronic communication is received when it comes to the attention of the addressee.

While this legislation is important in facilitating m-commerce, it will not improve the capacity of parties to authenticate m-commerce transactions.

---

[96] Reuters 2003, *Wireless Operators Lose Short Text Messages – Study*, 14 January 2003, http://www.reuters.com/ Accessed 16 January 2003

[97] Shiny new mobile technology 'suffers same old problems' *Sydney Morning Herald*, 30 June 2003

[98] Federal Trade Commission (U.S), 2002, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, February 2002, http://www.ftc.com p.19

The National Office for the Information Economy (NOIE), in 1999, established the National Electronic Authentication Council (NEAC) to oversee the development of a national regulatory and accreditation framework for the use of electronic authentication technologies. The Federal Government's *Gatekeeper* accreditation program for public key infrastructures (one authentication technology) was acknowledged by NEAC as a suitable standard for PKI implementations for Government applications. As a result of this work, Cabinet agreed that any future online digital signatures would need to be compliant with the Gatekeeper framework.

NEAC discussed whether this approach would be suitable for the private sector, but views of the Council were divided, and there has been no further consideration of a minimum standard of security that the private sector must adopt for electronic transactions. This matter is still being considered, in particular whether there is a need for specific Government action in relation to authentication technologies and the future applicability of the Gatekeeper framework for the private sector.[99]

There are no legislative requirements for the use of minimum security features or technologies for electronic transactions. Nor are there any such requirements for businesses to inform consumers of the potential security risks that arise in electronic transactions.

International regulatory responses

In 1999 the European Commission adopted a legal framework guaranteeing EU-wide recognition of digital signatures. The *Digital Signatures Directive*[100] defines the requirements for digital certificates and certification services to ensure minimum levels of security and allow their free movement throughout the EU. The Directive aims to facilitate the use of electronic signatures for online authentication and contribute to their legal recognition. Electronic signatures allow someone receiving data over electronic networks to determine the origin of the data and to check that that data has not been altered. They are defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".[101] The Directive also defines certain requirements for certification service providers to ensure a guaranteed minimum level of security.

The Directive is not designed to regulate everything in detail but defines the requirements for digital certificates and certification services so as to ensure minimum levels of security and allow their free movement throughout the Internal Market. Its main elements are:[102]

- the Directive stipulates that an electronic signature cannot be legally discriminated against solely on the grounds that it is in electronic form
- all products and services related to electronic signatures can circulate freely and are only subject to the legislation and control by the country of origin
- the legislation establishes minimum liability rules for service providers who would, in particular, be liable for the validity of a certificate's content
- the legislation provides for legal recognition of electronic signatures irrespective of the technology used (e.g. digital signatures using asymmetric cryptography or biometrics.)
- the legislation covers the supply of certificates to the public aimed at identifying the sender of an electronic message, and
- the legislation includes mechanisms for co-operation with third countries on the basis of mutual recognition of certificates and on bilateral and multilateral agreements.

Under the Directive on Privacy and Electronic Communications,[103] concerning online security and privacy, carriage service providers must inform customers of any security risks in transmitting data. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of

[99] The National Office for the Information Economy (NOIE), 2002, *Towards a National Authentication Framework: Discussion Paper, May 2002*, p7 http://www.noie.gov.au/projects/confidence/Improving/authentication.htm Accessed 15 November 2003

[100] *Directive 99/93 on Electronic Signatures*

[101] Baker & McKenzie, 2001, *op cit*. p 21

[102] European Commission, 2003, Data Protection Guide, http://europa.eu.int/comm/internal_market/privacy/index_en.htm Accessed 13 October 2003

[103] European Commission, 2002, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*

software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message.

Key issues for consideration

- **Should the Government have a role in implementing minimum security requirements for m-commerce transactions?**
- **What protections will be in place for a consumer if a mobile phone with commerce capabilities is lost? Who will liable?**
- **Should there be a requirement to inform customers of specific security risks associated with online wireless transactions? How far is this covered in the contract's terms?**

3.4.2 Protecting consumers from fraud

Description of the problem

A wide range of payment technologies exist and more are being introduced, all of them with the potential of being used in m-commerce. However, it has been found that there are still many issues that remain unclear to consumers regarding e-payments, including liability and the roles and responsibilities of parties intervening in an e-transaction if a security threat occurs.[104]

Information about the security of payment systems that are used to support electronic transactions could include:

- how e-merchants verify their customers' credentials
- whether buyers have the possibility to check the details of the payment ordered before execution
- whether and how payment has actually been performed, and
- how the e-payment system may prevent repudiation.

Consumers may be unaware of their liability risks using different electronic payment mechanisms, as well as their rights in an electronic payment and the sorts of problems and faults that may occur during an electronic payment transaction. Furthermore, consumers may not realise that losing a mobile device carries with it potential exposure to identity theft and fraud due to the level of personal information that is contained in these devices. Consumers also need to know how they can minimise the risk of unauthorised transactions or the impact of other security breaches.

Industry approaches to the issue

As discussed briefly above, in July 2003 the Australian Internet Industry Association released a draft Cybercrime Code of Practice that attempts to specifically deal with issues of cybercrime - crimes involving computers and electronic communications. This could effectively extend to m-commerce transactions. The objectives of the Code are to:[105]

- facilitate co-operation between ISPs and law enforcement agencies and establish clear policies and procedures for investigations
- provide a transparent mechanism for the handling of law enforcement agencies' investigations for the Internet industry and ensure both ISPs and law enforcement agencies understand the procedures
- promote positive relationships between law enforcement agencies and the Internet industry, and
- ensure that the privacy of users will be protected from unlawful intrusion by law enforcement agencies.

In drafting the Code, the IIA has attempted to balance the privacy issues with the need to improve security of Internet transactions and assist law enforcement agencies in curtailing criminal transactions over the Internet and other electronic mediums.

The Australian Bankers' Association has commenced work on three major projects aim at improving fraud prevention in all banking transactions, including face-to-face and electronic services. These include:

- the development of voluntary industry standards on security and fraud prevention

[104] Price Waterhouse Coopers (PWC) 2003, *Study on the security of payment products and systems in the 15 Member States, Final Report*, (Contract No. ETD/2002/B5-3110/C/11), 16 June 2003, http://europa.eu.int/comm/internal_market/payments/docs/payment-instruments/security/200309-finalreport_en.pdf. Accessed 20 October 2003

[105] Levinson, E. & Ceola, N. 2003, *op cit*.

- an analytical study of identity documents, and
- the development of a fraud education program for banking customers.

Recognising the potential for identity theft in the electronic environment, a group of financial services, information technology and electronic commerce companies and organizations have recently established the Coalition on Online Identity Theft, announced in September 2003. The Coalition states that it will work together to fight online identity theft through a variety of educational, legal and technical solutions to protect consumers and companies from online fraud, including:[106]

- expand public education campaigns against online identity theft to protect consumers and ensure that they can have confidence in Internet commerce
- help promote technology and self-help approaches for preventing and dealing with online identity theft
- document and share non-personal information about emerging online fraudulent activity to stay ahead of criminals and new forms of online fraud, and
- work with government to cultivate an environment that protects consumers and businesses, and ensures effective enforcement of criminal penalties against cyber thieves.

Current regulatory protections in Australia

As noted earlier, there are limited statutory protections in Australia's current regulatory framework to protect consumers against financial loss in electronic trade. Most protections are laid down in industry practice. The Commonwealth Government's *BPM for Electronic Commerce* identifies the following items that businesses should provide to protect consumers and themselves in conducting electronic transactions:

- easy to use payment mechanisms
- security that is appropriate to the transaction
- access to information on the security of payment and authentication mechanisms, and
- contracts that take account of their own responsibility for losses arising from the misuse or failure of authentication mechanisms.

International regulatory responses

The issue of legislating security requirements that support electronic transactions has been canvassed in the EU. There is, however, a general perception that harmonising legislation about the technical requirements related to the use of electronic payment systems cannot be the ideal solution. Technical solutions supporting e-payments vary across borders and it is recognised that the ideal of interoperability cannot be achieved, at least in the short term. It has been argued that the most realistic solution should be that legislators leave the actual market players to take the lead in introducing the best e-payment practices.[107]

PriceWaterHouseCoopers noted that Denmark has adopted specific legislation to regulate the time, form and quality of information that should be provided to consumers when using certain payment instruments, notably e-payment cards, in e-commerce transactions. The beneficial result for consumers is that all financial institutions and service providers in Denmark now communicate information regarding the security of electronic payment systems as a matter of course.

Key issues for consideration

- **Are consumers aware of the liability and responsibility of each party in the case of a security breach?**
- **Is there sufficient protection for consumers using complicated payment systems that may be vulnerable to fraud? Are consumers aware of how they can protect themselves?**

3.5 Content

Advanced mobile phones provide a potentially lucrative channel for content owners to sell their content, but there has to be a way for these developers to make choices about how that content is used and paid for.[108] Perhaps one reason that we have not seen the m-commerce content market develop as first expected is the issue of how creators can protect their content.

[106] ICT Outlook Forum, 2003, *Coalition Forming to Crack Down on Online Identity Theft*, Media Release. http://www.ictforum.com.au/releases/04bSept03.htm

[107] PriceWaterhouseCoopers (PWC) 2003, *Study on the security of payment products and systems in the 15 Member States, Final Report*, (Contract No. ETD/2002/B5-3110/C/11), 16 June 2003, http://europa.eu.int/comm/internal_market/payments/docs/payment-instruments/security/200309-finalreport_en.pdf. Accessed 20 October 2003

[108] Spender, L. 2003, Get the Message?, printed in *Australian Technology @ Business*, May 2003, Issue, p.15

It has been indicated that the value of content in television and other more traditional mediums will decline as people use the Internet and other multimedia related services such as messaging to access news, information, and entertainment. However, developers will need to invest in a system that prevents content being exploited and ensures that consumers pay for what they get.

The Open Mobile Alliance, a global alliance of handset manufacturers and telecommunications carriage service providers, has recently adopted a new rights management framework for controlling digital content usage on mobile handsets. The Open Digital Rights Language system, by way of example, will allow mobile users to send personal content to friends and colleagues as can already be done. However, it will also enable forward-locking of mobile content, preventing consumers from sending commercially valuable content such as information updates or sports clips to other users, unless the appropriate licence has been obtained from the content owner.[109]

While the issue of protecting content is not necessarily a consumer issue, it does have some important implications in determining how the content market will develop. A more relevant issue for consumer protection and digital content is how consumers, in particular vulnerable consumers, will be protected from a plethora of content that may not be suitable.

The discussion presented here does not attempt to cover any of the broader copyright issues that have been raised with the introduction of e-commerce and are likely to also apply to m-commerce.

3.5.1 Production of and access to adult content and pornography

Description of the problem

Pornography raises essentially the same concerns and interests in any medium. However, the capacity to have pornographic information accessed by and distributed to a mobile phone has a number of unusual features that affect the regulation of online pornography.

A related issue of mobile phones potentially being used for the creation, as opposed to the distribution, of child pornography through their capacity to take and transmit digital photographs has also been subject of some concern internationally.

Industry approaches to the issue

Technology is constantly and rapidly developing and has the potential to succeed in restricting access by particular classes of people to particular content. This could be done, for example, by requiring first time users to adult sites to pay a fee by credit card to ensure that they are adults and thereafter to access or purchase the content using a password. While such a system would contain some flaws – for example, where children learn their parents' passwords – on the whole it would be more effective in restricting children's access to pornography than, say, running late-night broadcasts is in restricting children's access to adult television.[110]

Mechanisms that allow access to adult content often rely on a logged-in membership system which asks the consumer to identify their date of birth at the time of registration. Only members identified as being over 18 are then allowed to access this content. Carriage service providers are examining ways of registering phones that are owned by those under 18 and certifying adult content through a classification scheme to make sure that such content cannot be accessed by those under 18. Other companies are looking at technology that would enable content providers to register adult content and allow parents to bar their children's phone from receiving such content.[111]

As mobile phone contracts are only available to persons over 18 years old, it could be argued that there is an added protection mechanism that only those persons who are over 18 will be accessing the content; however, the issue remains that a large number of parents purchase phones for their children and their use is not further regulated. Research shows that up to a quarter of Australia's 14 million mobile phone users are children. More than a third of those aged 10-15 have their own phone. Furthermore, the introduction of prepaid services are increasingly opening up the m-commerce market to young people.

[109] *ibid*.

[110] Voon, T. 2001, Online Pornography in Australia: Lessons from the First Amendment, University of NSW Law Journal, 2001 UNSWLJ 15

[111] Gibson, O. 2003, Mobile firms eye 'Playboy' services, *The Guardian*, Monday 13 January 2003. http://media.guardian.co.uk, Accessed 14 January 2003

In the UK, 3G carriage service providers have been looking at adult content as one way to recoup their massive investments.[13] A code of practice is being drawn up to head off concerns about material reaching minors.

Current regulatory protections in Australia

On 1 January 2000, the *Online Services Act*, Australia's approach to online pornography, came into effect. Under the Act, a new Schedule 5 was inserted into the *Broadcasting Services Act* 1992 (Cth), setting up a scheme for regulation of certain content on the Internet.

Under the *Online Services Act*, Internet content hosted in Australia may be the subject of a takedown notice by the Australian Broadcasting Authority (ABA). Such a notice directs the content host to cease hosting particular content and not to host it in the future. The classification of content for the purposes of the notice is based on the Australian classification scheme for films and television programs, which includes the categories of R (restricted), X (sexually explicit) and RC (refused classification). The ABA is required to issue take down notices in respect of content hosted in Australia that has been or is substantially likely to be rated X or RC. Unless subject to a restricted access system approved by the ABA, such as one that requires a PIN to access, content rated R is also prohibited.[112]

The *Online Services Act* also addresses Internet content hosted outside Australia and the ABA can similarly issue a notice to an Australian ISP to take reasonable steps to prevent access to prohibited or potentially prohibited content hosted offshore. For offshore content, the prohibition applies only to X and RC rated material. In late 1999, the ABA registered a code of practice developed by the Internet Industry Association allowing ISPs to provide end users with approved content filters rather than blocking content from overseas sites.

The provision of adult content over mobile phones is likely to come under the purview of the ABA; however, the extent to which the *Online Services Act* is robustly enforced has been questioned. Various commentators have criticised the Act as being ineffective in its goal of limiting access to pornography on the Internet and unduly onerous in imposing strict obligations on ISPs. Further criticisms have been voiced that while it ostensibly derives from a concern about children's access to such material, the Act makes no attempt to limit itself to children's access and restricts adult choices as well.

On 11 February 2002, the Commonwealth Minister for Communications released for comment proposed new Regulations (the *Telecommunications (Consumer Protection and Service Standards – Telephone Sex Services Regulations 2001*) relating to telephone sex services. These regulations have not been promulgated in Parliament and have introduced a registration scheme for telephone sex service providers, restrictions on advertising telephone sex services and new provisions relating to telephone sex services.[113]

In Victoria, the Victorian Attorney-General is calling for a national taskforce to tackle the use of mobile phone cameras and the publishing of indecent photographs of children on websites. The Attorney-General has stated that he will raise both issues at the Standing Committee of Attorneys-General meeting in Canberra.

International regulatory responses

In 1996, the US Congress created two criminal offences related to Internet content under the *Communications Decency Act* (CDA). The CDA provided that it was an offence to:

- initiate the transmission of an obscene or indecent communication by means of a telecommunications device, knowing that the recipient is under 18 years of age; or
- use an interactive computer service to send or display to a person under 18 years of age a communication that describes sexual or excretory activities or organs in terms that are patently offensive as measured by contemporary community standards.

The EU holds the content provider, including a retailer or the owner of the material that is being transmitted, fully responsible for its commerce offers and for any unlawful content contained in information transmitted to consumers. Only in exceptional circumstances will the content provider be in a position to argue that it had no active role in the selection or modification of such information and should, therfore, have no or only limited liablity for unlawful content.[114]

[112] Voon, T. 2001, *op cit*.

[113] *Ibid*.

[114] Baker & McKenzie, 2001, *Doing E-Commerce in Europe*, http:// www.bmck.com. Accessed 20 September 2003, p18

There has been some recognition of the potential to distribute and pay for adult content through m-commerce. Korea's Ministry of Information and Communication in December 2002 introduced a law that regulates the sending of pornographic advertisements through the Internet to mobile phones.

In Thailand, entertainment content providers are calling for the government to crack down on websites that offer downloads of pornographic picture messages, including images that can be downloaded to mobile phone screens[115].

In Japan, the popularity of Internet-enabled mobile phones has been claimed to have caused a rise in sex crimes involving minors. It has been argued that the use of Internet-enabled phones has increased access for minors to dating sites. Details of users are given out and victims have been contacted via their mobiles. It has been argued that of the 793 sex crimes committed through online dating sites, nearly four out of five have involved minors. In response, Japan passed broad laws regarding sex crimes, however the legislation does not stipulate the use of different technologies.[116]

On the issue of mobile phone cameras, and the transmission of unauthorised and potentially illegal data, the Italian Data Protection Commission has published strict rules governing the use of picture messaging and video on mobile phones. 3G phone users may only record images of people for personal use, must keep pictures in a secure place and anyone captured on film must be informed if their image is to be displayed on the Internet. The transmission of pornographic pictures is strictly forbidden.

The Korean government has also addressed this issue, and has ruled that, by 2003, domestic manufacturers of mobile phone cameras must ensure that mobile phones emit a loud, shutterlike click or noise when the camera is activated.[117]

Key issues for consideration

- **How well will current content laws apply to the increasing use of mobile phones to access and transmit inappropriate content?**

3.6 Summary

The review has found that m-commerce is likely to raise a number of issues and potential concerns for consumers. These extend far beyond the traditional fair trading issues, to encompass other issues such as privacy, security and content issues. Importantly, many of these issues will impact, not only on consumers, but also on merchants that are using m-commerce as another mechanism to broaden their reach to customers and support transactions.

The analysis presented above identifies the Commonwealth, State and Territory key legislative provisions for protecting consumers as they use m-commerce services.

The paper also identifies some of the industry-based initiatives that have developed in response to the increasing use of the Internet and other technologies. This includes codes of conduct to deal with the potential intrusiveness of direct marketing, practices to respond to the use of computers to conduct financial transactions, and protection mechanisms to deal with potential debt problems arising from the use of 1900 numbers. A number of these current industry-based responses will potentially have application to the roll-out of m-commerce services, and will provide some additional protection to consumers, beyond those prescribed in regulation.

Looking at the international approach to m-commerce, it appears that regulators around the world, while keeping a close watch on the way that m-commerce services evolve, are adopting a "wait and see" approach with regard to regulating these new services. There has certainly been no sustained effort to establish a series of new regulatory protections specifically in regard to m-commerce, and additional measures that have been put into place appear to focus on specific issues that have emerged in relation to these services rather than an over-arching regulatory response to m-commerce.

[115] Ed, 2003, Calls to tighten mobile content, *Bangkok Post*, 27 May 2003

[116] Ed, 2002, *Net-Linked Sex Crimes Involving Minors Up in Japan*, www.reuters.com, accessed 26 August 2002

[117] Ed, 2003, Camera-phones must "click" in Korea, *ZDNet*. 13 November 2003, http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20280927,00.htm

However, it is clear that m-commerce, as it develops, is likely to require new regulatory responses. M-commerce will enable consumers to undertake new and varied transactions that will not necessarily be covered by either existing legislation or industry-based approaches. Australian and international regulators alike will be confronted with these issues as the technology develops, and as m-commerce services proliferate.

It is essential that regulators continue to monitor developments to ensure a speedy response to emerging consumer issues as they arise.

“Section 4 Conclusion”

4

This project commenced in 2002, when the market for m-commerce services was only just developing. It was anticipated, at this time, that the market would mature very quickly, which, as identified in this paper, has not necessarily occurred.

In conducting the review it has become clear (a) that m-commerce services are currently only at an early stage of development and there is still significant uncertainty as to the services m-commerce will support and the features of these services; and (b) there are many agencies that will have a potential role in overseeing the introduction of m-commerce services.

Firstly, consultation with industry organisations has identified that there is still considerable uncertainty as to the way that m-commerce services will evolve. To a large extent, the capacity for m-commerce services to become an accepted alternative to other forms of shopping, including physical and electronic forms, will depend on the acceptability of the payment mechanisms that emerge, and the ability for operators to develop standard systems that will support interoperability. Other considerations, including the availability of content and services is another key factor in the development and uptake of m-commerce.

The review process has also identified that there are already a range of regulatory interventions that have been put into place that will potentially apply to m-commerce. Furthermore, as m-commerce services are developing, the industry is making some efforts to address key concerns for consumers. Engendering consumer trust in m-commerce is essential to drive uptake of m-commerce as an alternative purchasing and payment option.

While it cannot be presumed that it can be “left up to industry” to provide adequate consumer safeguards, any additional regulation needs to be considered in light of the current regulatory protections afforded by existing legislation and the various self-regulatory approaches that have been adopted by industry that will have application to m-commerce.

Secondly, agencies, including the ACA, consumer protection agencies including the ACCC and state and territory fair trading agencies, the Australian Privacy Commissioner and the Australian Broadcasting Authority (ABA) have begun to investigate their role in relation to supporting the development and uptake of m-commerce. The ACA has recently released a discussion paper on the issues arising from m-commerce and the Commonwealth’s E-Commerce Expert Group has been asked to consider m-commerce in its review of the Best Practice Model for E-commerce. This review is currently being undertaken. The benefits that m-commerce will potentially offer industry and consumers could be compromised if there is not effective communication between governments and regulators. There is the risk that separation of powers, not only between regulatory agencies, but between jurisdictional and national levels could result in either duplication of effort or inconsistencies in approach.

A co-operative approach between agencies is required to enable a full consideration of the issues raised by m-commerce and the development of a regulatory approach that will stimulate the development of the m-commerce industry in Australia while providing suitable safeguards to consumers, merchants and other users.

Next Steps

This paper provides a basis for considering whether any issues identified need to be further explored in order to support the uptake of m-commerce. It also asks whether there is a role for government in providing an appropriate regulatory framework to support the development and uptake of m-commerce service.

The paper will be circulated for consideration among stakeholders, including government agencies and regulators, consumer organisations, industry players and individuals. The SCOCA Working Group would be pleased to receive comments on the issues raised in this paper, and options to take this work forward.

It is proposed that, rather than embarking on Stage Two of this project, further work is put on hold pending discussions among regulators as to how to best examine m-commerce in a collaborative manner, and in a way that will avoid duplication of effort and research. It is essential that all players are involved, and that all issues are considered in determining the best way to respond to m-commerce.

The E-Commerce Working Party recommends that developments in m-commerce, including technological and market developments, as well as regulatory developments, both nationally and internationally, be closely monitored over the next 12 months. This will provide consumer protection agencies with a stronger basis upon which to determine the sorts of key issues that need to be addressed by government to protect consumers, and will also give regulators an opportunity to hold further discussions and explore the potential roles that different agencies could play to support the introduction and uptake of m-commerce in the Australian consumer market.

Recommendations of the Working Party

1. **That the Ministerial Council on Consumer Affairs agree to the public release of this report.**
2. **That the SCOCA E-commerce Working Party continue to monitor market and regulatory developments relating to m-commerce over 12 to 18 months from release of this issues paper.**
3. **That regulatory agencies continue to liaise regarding the issues being raised by m-commerce and consider the development of a regulatory approach that will provide suitable safeguards to users.**
4. **That a further report on m-commerce developments and issues be prepared for MCCA in 2006.**

Appendix: Emerging Applications

There are a range of products and services that are likely to be delivered and accessed using m-commerce applications. The following table identifies key features of the various types of m-commerce services that are currently available and are likely to emerge in the next few years.

M-commerce Service	What is it?	Availability and future trends
Purchasing telecommunications related products (e.g. ring-tones and games)	The download of custom telephone screen features and ring-tones onto the handset for ongoing use. Normally the charge is directly added to the phone bill. Game downloads and SMS competitions are also attracting greater attention.	A 2003 survey of around 1,000 mobile users by AMR Interactive found that 55 per cent of Australian mobile users were aware of their ability to download games to their handsets, but only 5 per cent said they were 'very interested' in doing so. Games are downloaded in the same way as ring-tones. For example, an average current mobile phone can house four to five games which cost as much as $15 each.
Instant payment for a non-telecommunications product (e.g. parking ticket, theatre ticket)	A consumer can use their mobile phone to pay instantly for either a service or product with the cost of the service or product added directly to the phone bill.	Trials are currently being conducted in Melbourne and Sydney where consumers can use their phones to pay for the cost of parking. USA Technologies, a US m-commerce company, is currently installing phone-equipped Laundromats in four major universities. Each of the washers and driers has a mobile phone with a 1800 number built into its control box. Students log into a website and then book and pay for their service through their phone. An added benefit for the universities is a reduction in vandalism because the machines have no money in them.

M-commerce Service	What is it?	Availability and future trends
Shopping	A consumer may purchase and arrange for delivery of physical products using a mobile phone.	Wireless shopping is currently available on WAP-enabled handsets which provide access to wireless websites. Purchases may be made using a credit card on WAP sites in the same way that e-commerce transactions take place. As carriers build wireless portals, shopping will also take place through the mobile service provider, who bills the customer on behalf of a third party. At present, there is almost no activity in either area in Australia and New Zealand. Slow network speeds, non-colour telephone screens, and complex, fiddly browsing have held back development of mobile shopping. This will change as faster networks and more advanced handsets come onto the market.
Mobile advertising	Personalised, broadcast, or location-specific advertising material may be sent directly to a telephone handset. It may also be embedded with free or fee-based information services.	To date, Australian marketers have concentrated on SMS sales promotions and competitions for companies such as Network Ten, Nova 96.9, Coca-Cola, and McDonalds. Promotions have also included 'm-coupons' for discounted products and services. Consumers either pull these m-coupons from the service provider's wireless portal as desired, or have several sent via SMS each day. Mobile advertising will eventually expand from text-based SMS marketing into pictures and video once a critical mass of consumers possess MMS-capable handsets. Location-based advertising will also be very attractive to marketers, although the variety of services and its spread may be limited by consumer concerns about privacy.
Information services	Consumers can register for wireless directory, news, and information services. These may be location-based messages, newscasts, video or music clips and may come via SMS, wireless e-mail, or be accessed on a website. The variety of text-based information services will only be limited by consumers' willingness to pay for information to be sent to their mobile phones. As more handsets become MMS-capable, information and entertainment will come as images, video, or may be read to the user over the phone. 3G could also bring streamed video and other information content. In the UK, researchers are already examining the potential of 'mid-air messaging' where information can be beamed to people carrying certain devices in the street.	Among the services already available are news, weather, stock quotes, sports scores, and traffic information. Such services may be subscription-based or advertising-supported. Initial payment is arranged on a website with a mobile service provider acting as biller for third party content provider, or directly through a content provider. Information services may also include database services that consumers can use to locate a shop or service, for example the address of a local chemist. In January 2003, Hutchison Essar announced the launch of HutchAlive, a personalised interactive broadcast service. The service delivers a wide range of text-based infotainment services that arrive on a subscriber's phone. Messages are delivered simultaneously to a large number of users. The consumer can activate or deactivate the service at any time, and it is delivered free, with the option of further information that is paid for. The service also delivers advertising and promotional offers.

M-commerce Service	What is it?	Availability and future trends
Locational based services	Mobile operators know where handsets connected to their networks are physically located at any particular moment. There are two main positioning strategies. Carriers can provide services to customers based on this information. Information services include maps, transport and merchant data. A third party would also be able to track the location of the handset owner from another I-Mode phone or an Internet-connected PC. An online shopping portal site will sell tracking and emergency-related GPS services.	Examples of location-based applications are: information and directions to the nearest gas station and navigational services to help avoid traffic congestion. Both indoor and outdoor locational services are envisaged. Indoor services could be offered in a shopping centre, where a consumer can receive real-time information based both on personal preferences and current position in the centre. By registering a shopping list in advance, the system could provide a suggested route to obtain the products on the list and enable special offers to be sent to the consumer as he shops, with the merchant able to target special offers to the consumer as he wanders by. Future services may expand to: highly targeted advertising services, roadside assistance, and emergency assistance. Location may also be used to determine billing; for example, to charge subscribers at a residential rate when they call from home. Growth of these types of services will depend on how well service providers protect privacy and provide a user-friendly experience.
Gambling	Consumers may be able to place sports bets, enter lotteries, or play games of chance using their mobile telephone handset.	As of early 2003, some 5 per cent of the TAB's racing turnover and 20 per cent of its sports betting was done online. Telephone betting is already popular.
Mobile banking	Electronic banking allows customers to remotely access bank account information, transfer funds and pay bills.	Until recently, mobile banking has been limited to the transfer of non-critical data like account information. This is now moving into full-blown transactions, such as shifting funds, and paying bills. Mobile banking will be further driven by banks' desire to reduce overheads. A service that has recently become available is Mobile EFTPOS. Telstra's Mobile EFTPOS service provides tradespeople and mobile workers with a special handset that can facilitate credit, debit and charge card transactions. This allows them to get paid on the spot. A similar service from Optus called *MobilePay* uses a mobile phone and a tamper-proof credit card swiper to verify payment.

M-commerce Service	What is it?	Availability and future trends
Entertainment services	Consumers can register for wireless chat, entertainment, video conferencing, picture and video messaging. Some of these services, especially messaging and video conferencing, are value-added mobile services, but they might fall outside the definition of m-commerce except in instances when the messaging is between a business and a consumer. A wireless purchase of the service, however, may be considered an m-commerce transaction.	Chat applications are already available. For example, Telstra began offering ICQ for SMS in February 2003. The service allows mobile telephones to send and receive ICQ instant messages from Internet users or other phone subscribers over SMS. Other chat and instant messenger services such as MSN Messenger are also now available on mobile phones. Current entertainment offerings include basic telephone handset features such as ring-tones, multiplayer video games, competitions, and music or video content. Higher bandwidth 2.5G and 3G networks are making interactive multimedia entertainment a reality. Entertainment content is likely to expand into picture, music and video downloads, including streaming content. Madonna and other artists already send text messages to mobile phones about new albums or tour dates. The US mobile music market for all content has been forecast to jump from US$50 million in 2003 to between US$400 million and US$500 million by 2007.

Glossary

1G
The first generation of analogue mobile phone technologies.

2.5G
The enhancement of GSM, which includes technologies such as GPRS.

2G
The second generation of digital mobile phone technologies, including GSM and CDMA.

3G
The third generation of mobile phone technologies, which has a much higher speed of data transmission than 2G. These higher speeds allow the transmission of video and two-way video telephony. Other data connections, e.g. download of information or JAVA applets, are also several times faster on 3G networks then on older 2G networks.

4G
The fourth generation of mobile phone technologies. 4G mobile communications will have higher data transmission rates than 3G, up to 20 megabits per second, which in principle will allow high-quality smooth video transmission.

ABA
Australian Bankers Association. The self-regulatory body established by the banking industry.

ABA
Australian Broadcasting Authority. The Australian Commonwealth Government body that monitors compliance with the ownership and control provisions of the Broadcasting Services Act, including the regulation of content on the Internet.

ACA
Australian Communications Authority. The government body that is responsible for regulating telecommunications and radio-communications, including promoting industry self-regulation and managing the radiofrequency spectrum. The ACA also has significant consumer protection responsibilities.

ACIF
Australian Communications Industry Forum. The self-regulatory body established by the telecommunications industry.

ADMA
Australian Direct Marketing Association.

ARPU
Average Revenue Per User.

ASIC
Australian Securities and Investment Commission. Commonwealth government body that enforces and regulates company and financial services laws to protect consumers, investors and creditors.

Authentication
The process that enables mobile phones and service providers to confirm the identity of any phone placing and receiving a call, allowing route of call, accurate billing and inhibiting unauthorized usage of the system.

Bandwidth
The width or capacity of a communications channel. Analogue bandwidth is measured in Hertz (Hz) or cycles per second. Digital bandwidth is the amount or volume of data that may be sent through a channel, measured in bits per second, without distortion. Bandwidth should not be confused with the term "band", such as a wireless phone that operates on the 800 MHz band. Bandwidth is the space it occupies on that band. The relative importance of bandwidth in wireless communications is that the size, or bandwidth, of a channel will impact transmission speed. Lots of data flowing through a narrow channel takes longer than the same amount of data flowing through a broader channel.

BFSO
Banking and Financial Services Ombudsman. Handles complaints made about the banking industry.

Bit
A bit is the smallest unit of information. As bits are made up using the binary number system, all multiples of bits must be powers of two i.e. a kilobit is actually 1024 bits and a megabit 1048576 bits. Transmission speeds are given in bits per second (bit/s)

Broadband
A term used to compare frequency bandwidth relative to 3 MHz narrowband frequencies. Broadband frequencies can transmit more data and at a higher speed than narrowband frequencies. In general, typical paging services utilise narrowband frequencies. Wireless phones and communication devices use broadband.

Call Barring/Call Restriction
Enables you to restrict or bar certain or all types of calls to and from your mobile phone, i.e. outgoing calls, outgoing international calls, incoming calls. Barring is activated with a personal code. To use this service, it must be supported by your network and by your phone. You may also have to add this service to your subscription.

CDA
Communications Decency Act. US legislation regulating obscene or indecent Internet content.

CDMA
Code Division Multiple Access (CDMA) is one of several digital wireless transmission methods that differentiates individual transmissions by assigning them unique codes before transmission. CDMA offers improvements over analogue transmission in the areas of reduced call dropping, battery power conservation, more secure transmission and increased service options. There are a number of variants of CDMA (see W-CDMA, for example).

CDR
Call Detail Records; the record made within the cellular network of all details of both incoming and outgoing calls made by subscribers, The CDR is passed to the billing system for action.

Cell
The geographic area encompassing the signal range from one base station (a site containing a radio transmitter/receiver and network communication equipment). Wireless transmission networks are comprised of many hexagonal, overlapping cell sites to efficiently use radio spectrum for wireless transmissions. Also, the basis for the term "cellular phone."

Circuit switching
A method used in telecommunications where a temporary dedicated circuit of constant bandwidth is established between two distant endpoints in a network. Mainly used for voice traffic; the opposite of packet switching.

COPA
Child Online Protection Act. US legislation that makes it an offence to knowingly, and for commercial purposes, make a communication to a minor by means of the Internet, where the communication is defined as obscene.

CSPs
Carriage service providers - telecommunications network operators.

Digital
A method of representing information as numbers with discrete values; usually expressed as a sequence of bits. Analogue information can be converted into a digital format.

EFT
Electronic Funds Transfer

FCC
Federal Communications Commission; the US regulatory body for telecommunications.

Frequency
The rate at which an electrical current alternates, usually measured in Hertz (Hz). Also the way to note a general location on the radio frequency spectrum such as 800 MHz, 900 MHz or 1900 MHz.

Gbit/s
A unit of data transmission rate equal to one billion bits per second.

GHz
A unit of frequency equal to one billion Hertz per second.

GPRS
General Packet Radio Service. GPRS represents the first implementation of packet switching within GSM, which is a circuit switched technology. GPRS offers theoretical data speeds of up to 115kbit/s and is an essential precursor for 3G.

GPS
Global Positioning System. A location system based on a constellation of US Department of Defence satellites. Depending on the number of satellites visible to the user, it can provide accuracies down to tens of metres. Now being incorporated as a key feature in an increasing number of handsets.

GSM
Global System for Mobile Communication. The second generation digital technology originally developed for Europe, but which now has in excess of 71 per cent of the world market. GSM was designed to provide the advantage of automatic, international roaming in multiple countries. The SIM (Subscriber Identification Module) card is a vital component in GSM operation, which enables the user to store all relevant data for the phone on a removable plastic card. The card can be plugged into any GSM compatible phone and the phone is instantly personalised to the user.

HTML
Hypertext Markup Language. A markup language developed specifically for web-based content.

I-Mode phone
Phone developed to display content written in HTML as in a traditional website.

Interworking
Systems or components, possibly from different origins, working together to perform some task. Interworking depends crucially on standards to define the interfaces between the components. The term implies that there is some difference between the components which, in the absence of common standards, would make it unlikely that they could be used together. For example, software from different companies, running on different hardware and operating systems can interwork via standard network protocols.

ISP
Internet Service Provider.

Mbit/s
Megabits per second. A unit of data transmission speed equal to one million bits per second.

MHz
Megahertz. A unit of frequency equal to one million Hertz.

MMS
Multimedia Messaging Service. An evolution of SMS, MMS goes beyond text messaging offering various kinds of multimedia content including images, audio and video clips.

MNO
Mobile Network Operator.

MPSA
Mobile Payment Services Association. Australian group of mobile operators developing a standardised payment system.

MVPN
Mobile Virtual Private Network.

NOIE
National Office for the Information Economy

Network
In the wireless industry, a network refers to the infrastructure enabling the transmission of wireless signals. A network ties things together and enables resource sharing.

NGN
Next Generation Networking. The next-generation network seamlessly blends the public switched telephone network (PSTN) and the public switched data network (PSDN), creating a single multi-service network. Rather than large, centralized, proprietary switch infrastructures, this next-generation architecture pushes central-office (CO) functionality to the edge of the network. The result is a distributed network infrastructure that leverages new, open technologies to reduce the cost of market entry dramatically, increase flexibility, and accommodate both circuit-switched voice and packet-switched data.

NPPs
National Privacy Principles. The 10 privacy principles that are included in the Australian Commonwealth *Privacy Act* 1988.

Packet switching
A communication system where the information is transmitted in packets of a set size. These packets have address headers and find their way to their destination by the most efficient route through the network. Compared to circuit switching where a connection is occupied until the traffic exchange is completed, packet switching offers considerable efficiencies as connections can be used by a number of users simultaneously.

PDA
Personal Digital Assistant.

PIN
Personal Identifier Number.

PKI
Public Key Infrastructure.

PSDN
Public Switched Data Network.

PSTN
Public Switched Telephone Network.

Roaming
A service unique to GSM which enables a subscriber to make and receive calls when outside the service area of his home network e.g. when travelling abroad.

SETEL
Small Enterprise Telecommunications Centre. National association advancing the telecommunications and e-commerce interests of Australian small business.

SIM Card
Subscriber Identity Module card. A smart card that must be inserted in any GSM-based mobile phone when signing on as a subscriber. It contains the telephone number of the subscriber, encoded network identification details, the PIN and other user data such as the phone book subscriber details, security information and memory for a personal directory of numbers. The card can be a small plug-in type or sized as a credit-card but has the same functionality. The SIM card also stores data that identifies the caller to the network service provider. A user's SIM card can be moved from phone to phone as it contains all the key information required to activate the phone.

SMS
Short Message Service; a text message service which enables users to send short messages (160 characters) to other users. A very popular service, particularly among young people, with 400 billion SMS messages sent worldwide in 2002.

SP
Service Provider.

SSL
Secure Sockets Layer. A security technology that is commonly used to secure server to browser transactions. This generally includes the securing of any information passed by a browser (such as a customer's credit card number or password) to a web server (such as an online store). SSL protects data submitted over the Internet from being intercepted and viewed by unintended recipients.

TIO
Telecommunications Industry Ombudsman. The independent dispute resolution service for consumers with complaints about their telephone or Internet service.

TPA
Trade Practices Act 1974 (Commonwealth)

VMNO
Virtual mobile network operator. A company that offers mobile services to customers using a third party's network.

WAP
Wireless Application Protocol; a standard for enabling mobile phones to access the Internet and advanced services. Users can access websites and pages which have been converted by the use of WML into stripped-down versions of the original more suitable for the limited display capabilities of mobile phones

W-CDMA
Wideband code division multiple access. A CDMA channel that is four times wider than the current channels that are typically used in 2G networks in North America. In January 1998, European Telecommunications Standards Institute (ETSI) decided to choose the W-CDMA technology to be the multiple access techniques for the third-generation mobile telephone system.

WML
Wireless Markup Language. A markup language developed specifically for wireless applications. WML is based on XML.

XML
eXtensible Markup Language. Similar to HTML, but where HTML describes content in terms of how it is to be displayed and interacted with, XML describes the content in terms of what data is being described.

Bibliography

Australian Communications Authority 9ACA), 2003, *Next Generation Networks: An ACA Perspective on Regulatory and Policy Issues*, ACA Contribution for Discussion ACIF NGN FOG Regulatory & Policy sub-group meeting, 20 May 2003.

ACA, 2003, Mobile Commerce, *Regulatory and Policy Outlook Discussion Paper*, August 2003 http://www.aca.gov.au

ACA, 2003, *Mobile Commerce Regulatory and Policy Outlook Discussion Paper: Summary of submissions*. October 2003, http://www.aca.gov.au

ACA, 2003, *ACA welcomes anti-spam bill*, Media release no. 57, 2 December 2003

ACT, 2003, Fair Trading Act 1992 (section 28A), http://www.legislation.act.gov.au/a/1992-72/default.asp

Allen Consulting Group, 2003, *Australian Mobile Telecommunications Industry: Economic Significance*, September 2003, Research Commissioned by the Australian Mobile Telecommunications Association, AMTA.

AT Kearney, 2002, *Mobinet Index # 4*, February 2002, http://www.atkearney.com http://www.atkearney.com

Australian Communications Industry Forum (ACIF) 2003, *Industry Code – Credit Management*, ACIF April 2003.

ACIF, 2002, *Short Message Service (SMS) Issues, Industry Code* ACIF C580:2002., August 2002

ACIF, 2003, *Billing: Industry Code*, February 2003.

Australian Direct Marketing Association (ADMA), 2001, Direct Marketing Code of Practice, http://www.adma.com.au, November 2001, p.10

ADMA, 2003, M-Marketing Code of Practice, http://www.adma.com.au, June 2003

ADMA, 2003, *Discussion paper regarding the need for additional regulatory measures in relation to the supply of premium services*, Submission to the ACA inquiry, http://www.aca.gov.au/aca_home/issues_for_comment/discussion/ comments.htm accessed 13 September 2003.

Baker & McKenzie, 2001, *Doing E-Commerce in Europe*, http:// www.bmck.com. Accessed 20 September 2003

Bennet, B. 2002, High delivery costs stifle realisation of 3G promise, *The Age*, 21 May 2002, p 5 NEXT.

Bond, K. & Turnbull, E., 2001, 'Meeting the Challenge of GPRS Billing', Analysis.com

Brightmail, 2003, *Spam Statistics: Spam Percentages*, www.brightmail.com/spamstats.html. Accessed 12 December 2003

Budde, P. 2003. *fromPaulsDesk*, http://www.budde.com.au.

Cahners In-Stat, 2002, [Online}, Available: http://www.instat.com/ [12 September 2002].

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

California, 2001, Public Utilities Code, http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=puc&codebody=&hits=20 [09 October 2002]

Cawdhry, P. and 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, 22 August, 2002.

Chidi, G., 2002, 'Forging circles of trust', InfoWorld 19 April 2002. [27 September 2002]

Christensen S. (2001) Formation of Contracts by Email – Is it Just the Same as the Post?, *QUT Law & Justice Journal*, QUTLJJ 3 2001. http://www.austlii.edu.au/au/journals/ QUTLJJ/2001/3.html#fnB7

Clarke, I., 2001, Emerging value propositions for M-commerce *Journal of Business Strategies*, pp. 133-148.

Clyde, I. 2003, *Click Here for Details: E-commerce and Consumer Credit*, Paper prepared for the Uniform Consumer Credit Code Management Committee, September 2003

Department of Communications, Information Technology and the Arts (DCITA), 2002, A Users' Guide to Australian Telecommunications, 12 November 2002 http://www.dcita.gov.au/Article/0,,2_3-3_143-4_112188,00.html

Dogac, A. and Tumer, A. 2002, Issues in mobile electronic commerce *Journal of Database Management*, Hershey, pp.36-42.

Durlacher, 2002, UMTS Report, http://www.durlacher.com/downloads/umtsreport.pdf, 27 August, 2002

Economist, 2002, 'Let Europe's Operators Free, Economist Newspaper, 26 September 2002

Ed, 2002, Mobiles call on gamers, *MX*, Thursday 6 June 2002

Ed, 2002, *Net-Linked Sex Crimes Involving Minors Up in Japan*, www.reuters.com, Accessed 26 August 2002

Ed, 2003, Camera-phones must "click" in Korea, *ZDNet*. 13 November 2003, http://www.zdnet.com.au/newstech/communications/story/0,20000

Ed, 2003, Phone me the money, *The Economist*, Mar 13th 2003, http://www.economist,com/displaystory.cfm?story_id=1633316 Accessed 20 April 2003

Engel-Flechsig, S. 2001, Securing the new global economy, Mobile Commerce World. http://www.mobilecommerceworld.com, accessed 18 August 2002

Ericsson, 2002, Consumers have moved beyond voice ... forever, www.ericsson.com . . Accessed 24 September 2002

EUPOlitix.com, 2003, *Banks to foot consumer protection bill*, http://www.eupolitix.com/EN/News/ff7df681-b4e4-4471-b70f-6e79bff8c923.htm

European Commission, 1007, *Directive 97/7 of the European Parliament and of the Council of20 May 1997 on the protection of consumers in respect of distance contracts (O.J. L 144, 04/06/1997)*

European Commission, 2002, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*

European Commission, 2003, *Data Protection Guide*, http://europa.eu.int/comm/internal_market/privacy/index_en.htm Accessed 13 October 2003

European Union, Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, *Official Journal of the European Communities 9/10/2002*

Federal Trade Commission (FTC – U.S), 2002, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, February 2002, http://www.ftc.com

FTC, 2002, E-commerce and the Internet, http://www.ftc.gov/bcp/menu-Internet.htm Accessed 10 October, 2002

Frost & Sullivan 2001, Briefing On: Digital Signatures, Biometric Identification, Andand Security

Gartner Group, 2001, *'Learning From the Success of NTT DoCoMo's i-mode'*, TU-14-0604, 9 July 2001

Gartner Group, 2002, *U.S. M-Commerce Market: Slow to Develop*, M-14-5621, 31 October 2002

Gibson, O. 2003, Mobile firms eye 'Playboy' services, *The Guardian*, Monday 13 January 2003. http://media.guardian.co.uk, Accessed 14 January 2003

Gosh, A. K., and Swaminatha, T.M., 2001. Software Security and Privacy Risks inMobile E-Commerce, Communications of the ACM

Government of the United Kingdom, 2003, *Communications Act* 2003, http://www.legislation.hmso.gov.uk/acts/acts2003/20030021.htm

Harter, B. 2001, Merging Markets, *Wireless Review*, 1 September 2001

Heath, M. and Wingfield, T. 2001, 'The m-Commerce Rainbow' www.kpmg.co.uk/kpmg/uk/image/mcom9.pdf Accessed 1 October 2002

ICT Outlook Forum, 2003, *Coalition Forming to Crack Down on Online Identity Theft*, Media Release. http://www.ictforum.com.au/releases/04bSept03.htm

IDATE, 2001, *Mobile Internet Uptake*

IDC, 2002, *Asia-Pacific M-Commerce Forecast and Analysis – Opportunities Await*, October 2002

KPMG Consulting, 2001, http://www.mcommcentral.com/documents.asp?grID=165&d_ID=397 Accessed 30 September 2002

Leaung, K. and Antypas, J., 2001, Improving returns on M-commerce investments, *The Journal of Business Strategy*

Levinson, E. & Ceola, N. 2003, Cybercrime Code of Practice for ISPs, *Internet Law Bulletin*, Vol 6, No. 5 2003

Levinson, E. & Ceola, N. 2003, *op cit*.

Lia Timson, 2003, Phones that make you go mmm, *The Age*, 9th September

Minister for Communications, Information Technology and the Arts, Senator Richard Alston, (2003), *Australian Government to Ban Spam*, Media Release, 23 July 2003, http://www.noie.gov.au

Minister for Consumer Affairs, 2003, *Victorian Consumers Face Problems Shopping Online*, Media Release, Tuesday, 11 March 2003. http://www.consumer.vic.gov.au

MMA, 2002, M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising

Mobile Metrix, 2002, *The Saviour of 3G – 2nd edition – An Analysis of the Leading Mobile Application and Content Providers*, Sweden

Monash University, *Monash Magazine*, Autumn/Winter 2003, Issue 11, 2003

NSW Office of Fair Trading, 2003, *Youth Debt: A Research Report*, prepared for NSW Office of Fair Trading by Daugar Research. November 2003

Nicholas, K. 2002, Telstra to market mobile credit pay units, *Australian Financial Review*, Saturday 5 October 2002

Nohria, N and Lesstma, M. 2001, A moving target: The mobile-commerce customer, *MIT Sloan Management Review*

Nokia, 2002, What is 3G? http://www.nokia.com/networks/systems_and_solutions/whatis_main/ 1,23779,1,00.html, Accessed 24 September, 2002

NOP World and Mobile Metrix study quoted at http://www.mcommercetimes.com/Technology/317

OECD Directorate for Science, Technology and Industry, 2003, *Report on Consumer Protections for Payment Cardholders*, Committee on Consumer Policy, 14 June 2002

Optus Newsroom, 2003, *A picture tells a thousand words*, 12 August 2003, http://www.optus.com.au. Accessed 22 August 2003

Ovum, 2002, *Mobile e-Commerce Market Strategies*, Ovum research paper

Ovum, 2002, *M-Payment: The second stage of m-commerce*, Ovum research paper.

Price Waterhouse Coopers (PWC) 2003, *Study on the security of payment products and systems in the 15 Member States, Final Report*, (Contract No. ETD/2002/B5-3110/C/11), 16 June 2003, http://europa.eu.int/comm/internal_market/payments/docs/payment-instruments/security/200309-finalreport_en.pdf. Accessed 20 October 2003

Price Waterhouse Coopers (PWC) 2003, *Study on the security of payment products and systems in the 15 Member States, Final Report*, (Contract No. ETD/2002/B5-3110/C/11), 16 June 2003, http://europa.eu.int/comm/internal_market/payments/docs/payment-instruments/security/200309-finalreport_en.pdf. Accessed 20 October 2003

Privacy Amendment (Private Sector) Act 2000, Commonwealth Government

Probe Research, 2001, *Wireless Internet Services, A CISS Bulletin, Defining the M-Commerce & Value ChainM, M-Commerce Business Models*, Vol. 2, No. 3 – 2001

Raisinghani, M. 2002, Mobile commerce: Transforming the vision into ,reality, *Information Resources Management Journal*, Hershey

Raisinghani, M. 2002, Mobile commerce: Transforming the vision into reality, *Information Resources Management Journal*

Reserve Bank of Australia, 2003, *Reform of Credit Card Schemes in Australia*, Media Release 19 September 2003, http://www.rba.gov.au/MediaReleases/mr_03_12.html

Reuters 2003, *Wireless Operators Lose Short Text Messages – Study*, 14 January 2003, http://www.reuters.com/ Accessed 16 January 2003

Sainsbury, M. 2002, Telco CFO Hangs Up On 3G Play, *The Australian*, 07 September 2002

Schema, *3G in Australia*, http://www.schema.co.uk/Assets_pubs/3G%20in%20Australia.pdf

SCOCA E-commerce Working Party, 2003, *Online Shopping and Consumer Protection*

Senator the Hon Ian Campbell, *M-commerce comes under expert group's eye*, Press release No. 12, 13 March 2003. http://parlsec.treasurer.gov.au Accessed 20 March 2003

Shiny new mobile technology 'suffers same old problems' *Sydney Morning Herald*, 30 June 2003

Siau, K., Lim, E. and Shen, Z. 2001, Mobile commerce: Promises, challenges, and research agenda, *Journal of Database Management*

Singtel sees strong demand for corporate SMS communications services, SingTel press release, June 2003

Spender, L. 2003, Get the Message?, printed in *Australian Technology @ Business*, May 2003, Issue, p.15

Stéphan Le Goueff, 2002, Resolution of Consumer disputes in the Digital World: *Desperately Looking for Confidence*, http://www.vocats.com

Strategy Analytics, 2002, *MobiPay System Winning M-commerce Implementation Race*, July 2002

Strategy Analytics, 2002a, Wireless Internet Applications,August 2002

Strategy Analytics, 2002b, Wireless Opportunity Analysis,June 2002

Strategy Analytics, 2002c, *MobiPay System Winning M-commerce Implementation Race*, 24 July 2002

Telecommunications Industry Ombudsman (TIO), 2003, *Telco credit management practices remain a cause for concern*, TIO Media Release, Thursday 9th October 2003

Telstra, 2001, *Wireless/work*, October 2001

Telstra, 2002, Pay for Parking, http://www.telstra.com.au/mobilenet/cur_prom/dialpark.htm Accessed 10 September, 2002

Thank, D. 2000, Security Issues in Mobile Commerce, *Proceedings of the Ist 1st International Conference on Electronic Commerce and Web Technologies*

The National Office for the Information Economy (NOIE), 2002, *Towards a National Authentication Framework: Discussion Paper*, May 2002 http://www.noie.gov.au/projects/confidence/Improving/authentication.htm Accessed 15 November 2003

Uul, N and Jørgensen N. 2002, Security Issues in Mobile Commerce using WAP, *15th Bled Electronic Commerce Conference*

van Heijden, Han, 2002, *Factors Affecting the Successful Introduction of Mobile Payment Systems*, Paper presented at the 15th Bled Electronic Commerce Conference: eReality: Constructing the eEconomy, Bled, Slovenia, June 17-19, 2002

Varshney, U. and Vetter, R., 2000, Emerging Mobile and Wireless Networks (Technology Information), *Communications of The ACM*

Voon, T. 2001, Online Pornography in Australia: Lessons from the First Amendment, *University of NSW Law Journal*, 2001 UNSWLJ 15

Vrechopoulos, A. et at, 2002, *Critical Success Factors for Accelerating Mobile Commerce Diffusion in Europe*, 15th Bled Electronic Commerce Conference, E-Reality: Constructing the eEconomy, Bled, Slovenia, June 17-19 2002

Which? *Online Annual Internet Survey 2002*, http://www.which.net/surveys/

Wireless World Forum, 2002, *mobile payments – making mobile services pay*, London

Wireless@KTH, 2002, *Wireless Foresight, Scenarios of the Mobile World 2015*, Sweden

Yorulmaz, T. and Ragas, D. 2002, The m-commerce roadmap, *AFP Exchange*, Bethesda

Yorulmaz, T. and Ragas, D. 2002, The m-commerce roadmap, *AFP Exchange*, Bethesda

ZDNet, 2002, Australians leading the world as m-banking wannabes, http://www.zdnet.com.au/newstech/communications/story/0,2000024993,20265553,00.htm Accessed 15 August 2002

Notes