ภาคผนวก ข

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY COMMITTEE ON CONSUMER POLICY, MOBILE COMMERCE (DSTI/CP(2006)7/FINAL), 16-Jan-2007

Unclassified **DSTI/CP(2006)7/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **16-Jan-2007**

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY

DSTI/CP(2006)7/FINAL
Unclassified

MOBILE COMMERCE

JT03220432

English - Or. English

FOREWORD

At its 72nd Session on 26-27 October 2006, the Committee on Consumer Policy (CCP) agreed to declassify the report by written procedure, which was completed on 22 December 2006.

This report was prepared by Mr. Yoshiaki Takahashi of the OECD's Secretariat Directorate for Science, Technology and Industry as part of the CCP work (www.oecd.org/sti/consumer-policy). The report is published under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

MAIN POINTS 4

INTRODUCTION 5

I. BUSINESS TRENDS AND DEVELOPMENT OF MOBILE SERVICES 10

II. TECHNOLOGICAL DEVELOPMENT 17

III. CONSUMER PROTECTION CONCERNS 21

IV. PRIVACY AND SECURITY ISSUES 33

CONCLUSION 41

APPENDIX A: PROVISION OF COMMERCIAL 3G SERVICES IN OECD COUNTRIES (AS OF SEPTEMBER 2006) 43

APPENDIX B: INTERNATIONAL ORGANISATIONS FOR MOBILE COMMERCE 45

APPENDIX C: COMPARATIVE TABLE FOR CONSUMER PROTECTION LAWS ON MOBILE COMMERCE 48

APPENDIX D: OECD STUDY ON MOBILE CONTENT (OECD (2005C)) 51

BIBLIOGRAPHY 53

MAIN POINTS

Developments in mobile handset technology and use of mobile devices by consumers have made the mobile commerce market more consumer-oriented, more global in scope and more device-dependent. As a result, consumers can reap the benefits of their handsets or other mobile devices at any time, anywhere. However, mobile commerce also raises some serious consumer policy issues such as the limited information available on screens and the security of payments made via mobile devices. Furthermore, the high penetration of such devices among minors may create serious risks of over-consumption and access to inappropriate content. To develop a healthy mobile commerce market, consumer policy makers and businesses need to promote its advantages while reducing the risk of potential disadvantages.

The mobile commerce market, which includes ringtones, music, games, video and other information services, is still in its infancy. Its level of development varies widely across OECD member countries. However, as mobile commerce takes off, the size of the market will increase exponentially because of network externalities.[1] Research companies see mobile commerce developing significantly in the future. The rollout of third-generation (3G) mobile services vastly increases the data transfer rate and therefore the variety of services that can be provided on a mobile device. New technologies permit mobile phones to be used as payment devices not only for virtual but also real-world shopping. New services, such as mobile digital television, location-based services and integrated financial services, are being offered by many market players. The cross-border use of mobile handsets for mobile commerce also has huge potential.

To ensure further development of the mobile commerce market, it is important to address consumer concerns. Technological developments have provided some solutions for challenges to the development of mobile commerce. However, along with these technological developments, other important measures are needed, including legal protection by governments, self-regulation by business and consumer information campaigns.

Some member countries are already tackling consumer policy issues, especially unsolicited sales, inadequate disclosure of information and protection of minors. Unauthorised use and SMS spam are also issues. However, action has been gradual and varies widely among OECD members. In terms of the legal framework, most countries currently apply existing laws or measures to mobile communications; few laws or measures specifically address mobile commerce. In addition, specialised information materials concerning the protection of minors are widely available for consumers.

Consumer officials in member countries evaluate consumer protection in mobile commerce quite differently. Some find that existing laws and policies cover most issues adequately, while others believe that more tailored responses are needed. Therefore, the Committee on Consumer Policy will continue to look closely at mobile commerce issues as the market develops and assess whether further activities should be undertaken to ensure that consumers are adequately protected on this new commercial platform.

---

[1] Network externalities are defined as the effects on a user of a product or service of the use of the same or compatible products or services by others (*e.g.* other family members and friends). It is usually said that a network industry such as mobile communication has positive externalities because the benefit of a user increase with the number of other users.

INTRODUCTION

Why is mobile commerce an important consumer policy issue?[2]

It is more consumer-oriented, more global in scope, more device-dependent.

Mobile commerce (m-commerce) can be understood as a business model that allows a consumer to complete all steps of a commercial transaction using a mobile phone or personal digital assistant (PDA) rather than by going to a "bricks and mortar" store or making voice calls.[3] Transactions involving the purchase of physical goods, such as books, that are delivered off line are still considered mobile commerce.

Technology experts predict that by 2020 mobile wireless communications are very likely to be available to anyone anywhere on the globe at extremely low cost (Pew Internet & American Life Project, 2006b). However, it is crucial to create and maintain consumer satisfaction and trust and reduce risks for consumers.[4] This is especially true when cross-border consumption is involved, as lack of familiarity with foreign policies and systems makes it more difficult for consumers to know their rights and use mobile devices easily. Mobile commerce is an important consumer policy issue for the following reasons.

First, most mobile users are *individuals*. Handheld devices are personalised and unlikely to be shared with others. Potential mobile commerce customers are also likely to be consumers. In Japan, 85.9% of mobile holders are individuals.[5] In France, 91.7% of all mobile holders use their mobile only for private purposes (only 3% use them only for business purposes) (AFNOM and TNS Sofres, 2005). The most striking phenomenon in member countries is the daily use of such devices by children and young adults. In a Norwegian survey, 80% of 8-24 year-olds answered that they had used a mobile telephone on the

---

2 Policy makers should also consider whether switching costs exist or not, as these can affect consumers' incentives to change the network services providers though it is not discussed in this report. In addition, because the Committee agreed that this project limited the scope which does not include issues relating to voice call pricing and messaging tariffs by mobile carriers, this report does not examine these issues.

3 The OECD's broad definition of an "electronic commerce transaction (e-commerce)" is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, or other public or private organisations, conducted over computer-mediated networks. The goods or services are ordered over such networks, and payment and ultimate delivery of the good or service may take place on line or off line (OECD, 2005f, Figure 3). In this sense, m-commerce is part of e-commerce. However, because new technologies make mobile phones potential payment tools not only for virtual shopping but also for traditional "bricks and mortar" shopping, they have some different characteristics.

4 Dr. Andreas Gentner of Deloitte pointed out at the CCP forum on mobile commerce in March 2005 that a win-win relation between consumers and service providers is the principle for success for mobile commerce. Empirical research on this point is relatively recent. Lin and Wang (2005) have examined a mobile commerce customer loyalty model. Also, Wu and Wang (2005) find that fear of the risks, for instance, involved in purchasing goods and services, has a significant effect on willingness to engage in mobile commerce.

5 Individual holders are estimated as the percentage of individuals with mobile or Personal Handyphone System (PHS) devices multiplied by Japan's total population. The percentage is provided in Ministry of Internal Affairs and Communications (MIC), Telecommunications Usage Trend Survey. Total population is estimated from MIC's basic resident registers.

previous day.[6] In Korea, more than 60% of those under age 19 have a mobile phone.[7] In Canada, 23% of students report having their own mobile phone, 44% of which have Internet capability (Media Awareness Network, 2005). In Japan, 11.8% of Grade 5 students (age 10-11) and 35.9% of Grade 8 (age 13-14) have their own mobile devices (National Congress of Parents and Teachers Association of Japan, 2005).[8] In France, 94% of 15-17 year-olds reported having mobile phones (AFNOM and TNS Sofres, 2005).[9]

Second, third-generation (3G) mobile services can be provided in many countries at *high data transfer rates*.[10] This platform provides converged voice, video, data, Internet and multimedia services. Given the compatibility of the systems used in different countries, when these services are available on mobile phones they are available over a broader geographical area. The number of subscribers to 3G services has recently begun to accelerate (Table 1). According to Strategy Analytics (2006), there will be more 3G than 2G subscribers by the end of 2006 in North America and by 2008 in Western Europe.[11]

Table 1. **3G subscribers, 2006**

System	Number of countries	Number of subscribers
cdma2000	72 (mainly America, Asia)	275.2 million
W-CDMA	55 (mainly West Europe and Japan)	70 million
HSDPA (3.5G)	36	N.A.

Source: The figures for cdma2000 are from the CDMA Development Group (CDG) and are for June 2006. The figures for W-CDMA and HSDPA are from the Global Mobile Suppliers Association (GSA) and are for September 2006.

Third, new technologies make mobile phones potential payment tools *not only for virtual shopping but also for bricks and mortar shopping*. This blurring of boundaries between the virtual and the physical world raises new consumer policy issues. Table 2 shows the differences in the technological infrastructure for web-based e-commerce and m-commerce. In particular, because the platform for mobile commerce is

6 Survey by SAFT (Safety, Awareness, Facts and Tools) (www.saftonline.no). Another survey by Telenor, Norway's largest provider of telecommunications services, shows that 100% of 16 and 17 year-olds had their own devices.

7 Total number of subscribers under age 19 for the country's three mobile carriers (SK Telecom, KTF and LG Telecom). Information provided by the Ministry of Information and Communication. Because parents sometimes sign mobile phone contracts for their children, actual numbers may be much higher.

8 Mitsubishi Research Institute (2006) confirms this trend. According to its survey, 11.2% of Grade 1-3 students (age 6-9), 21.1% of Grade 4-6 students (age 9-12), 49.5% of junior high school students (age 12-15), and 94.2% of senior high school students (age 16-18) had their own mobile phones in January 2006. A consulting firm, Wireless World Forum, estimated in February 2005 that penetration among children aged 5-9 years in Japan would reach 65% in 2007.

9 They answered that they used it to listen music (38%), to search sites (31%) and to participate into chatting (9%).

10 A 3G system can transfer 384 bps compared with 28.8 bps in 2G. An analysis of the development of 3G mobile services in OECD countries can be found in OECD (2004a). See also Annex A.

11 For example, SFR, a French mobile operator, had over 1 million subscribers in January 2006 who had downloaded 1.2 million television sessions in 2005. According to a survey by Ipsos Insight (2006), in 2005 45% of Japanese users, 31% of Korean, 20% of American, 19% of Canadian, 19% of British and 18% of French had used the Internet via mobile phones in the previous 30 days (for 2004, the corresponding figures were 54%, 28%, 20%, 14%, 13%, and 9% respectively).

device-dependent, the consumer can be identified.[12] This raises concerns about limited size of screen and personal identification, but it also leads benefits of anytime-anywhere use and to convenient and attractive new services offering because of mobility, seamless accessibility and flexibility.[13] As confidence in mobile commerce develops, such tools will be used more.

Table 2. **Differences in technological infrastructures**

Factors	Web-based commerce	M-commerce	U-commerce
Network infrastructure	1. Wired networking	1. Mobile/wireless networking	1. Ubiquitous networking
	2. Connectionless-based	2. Connection-based	2. Connection-based
	3. Data-oriented network	3. Voice-based network	3. Remote control technique
	4. Internet channel	4. Mobile phone network channel	4. Multicast channel
	5. Unlimited bandwidth	5. Limited bandwidth by spectrum	5. Broadband network
	6. Standards: TCP/IP	6. Standards: CDMA, TCP/IP(v6), Bluetooth, 3G	6. Standards: N/A
Application platform	1. Desktop computing	1. Mobile phone	1. Mobile computing and pervasive computing
	2. Device-independent	2. Device-dependent	2. Cross-platform
	3. General programming tools	3. Specific development tools	3. Specific development tools
	4. Easy to integrate with other systems	4. Difficult to integrate with other systems	4. Seamlessly integrates with other systems
Devices	1. Computing-centric	1. Communication-centric and computing-centric	1. Communication-centric and computing-centric
	2. Stationary location	2. Mobile location	2. Ubiquitous location
	3. Dominated by PCs	3. Dominated by handheld devices	3. Heterogeneous device
	4. Powerful CPU, large memory, big screen	4. Limited CPU, small memory, small screen, and slow bearers	4. Combination of handheld devices and remote control devices
	5. Full input model	5. Limited input model	5. Multiple input model
	6. Position may not be identified	6. Positioning and user identity capability	6. Geo-positioning and remember capability

Note: "U-commerce" means ubiquitous commerce. In the ubiquitous computing environment, every computer-embedded device is seamlessly connected to other devices in a broadband channel.

Source: Wu and Hisa (2004), "Analysis of e-commerce innovation and impact: a hypercube model", *Electronic Commerce Research and Application*, Table 1.

What are the advantages/disadvantages of mobile commerce for consumers? Why are consumers reluctant to engage in it?

All consumer goods and services present advantages and disadvantages. According to a survey in Japan (Mitsubishi Research Institute and Rakuten, 2003), users, and especially frequent users, of mobile commerce pointed out as advantages the ability to engage in mobile commerce anywhere and at any time (90.6%), followed by ease of finding goods or services (21.9%) and ease of handling an order (21.9%). A

12 Mahatanankoon *et al.* (2005) mention that one of the main features of mobile commerce is identifiability with "always on", location-centric, convenience and customisation.

13 However, if mobile carriers integrate mobile services vertically and then control the mobile commerce market, flexibility would be lost. If they do not block access to the Internet via a mobile handset, 3G (or more advanced) technology will allow consumers to access a wider variety of content through Internet sites than the mobile services provided by mobile carriers. Regulators will need to take such competition issues into account.

Korean survey (KCPB, 2002)[14] also highlighted the ability to use mobile commerce at any time and anywhere (45.9%). [15]

The greatest disadvantages mentioned by frequent users in the Japanese survey were the small screen (71.9%) and the limited amount of information displayed (50.0%). For infrequent users, security is also a big concern (48.7%). In a YouGov survey commissioned by Netonmy in the United Kingdom, 79% of consumers also felt that mobile services were becoming more complicated to understand and configure. This suggests that ease of use is also an important issue.

Furthermore, the high penetration of these devices among minors raises specific issues for mobile commerce. Children and young people use mobile phones as an essential part of their daily lives. Parents have some incentives to allow children to have mobile phones. For example, according to a February 2005 survey by the Survey Research Center, 56.7% of Japanese parents responded that the ability to check where their children are located in an emergency is the most important reason for allowing them to have their own mobile phones. According to another Japanese survey (Cabinet Office, 2006), 43.9% of parents also mentioned the ability to contact their children as a reason.

On the other hand, parents have some concerns about the use of mobile phones by children.[16] One reason, according to a survey undertaken by the New South Wales Office of Fair Trading in Australia, is that mobile phones, along with credit cards, are a potential source of debt for parents with children under 18 (NSW Office of Fair Trading, 2003, p. 18). An Austrian survey reveals similar concerns: 73% of parents with a child or children in school consider that their children's use of mobile phones presents the greatest danger of insolvency, far more than a car (54%) or the Internet (43%).[17] Also, according to a 2004 survey by Mobilkom Austria, 59% of children aged 10 to 14 do not know the difference between toll-free numbers and premium call numbers; 79% do not recognise the risks of SMS advertisements, which can lead to high mobile phone charges. These survey results suggest that regulators and businesses need to ensure whether the general rules for consumer contracts involving minors, which are mainly found in the Civil Code, also apply to transactions over mobile handsets involving minors who need to be treated differently from adults (see Section 5 of Part III in this report).

Therefore, to establish healthy mobile commerce markets, businesses and consumer policy makers need to consider how to promote the advantages while reducing the risk of disadvantages. The OECD Committee on Consumer Policy (CCP) started to examine consumer policy issues associated with mobile commerce in October 2004 and conducted a survey of member countries on this issue in 2006. A forum involving experts, the industry and consumers was also held in March 2005. The OECD Committee for Information, Computer, and Communication Policy (ICCP) also deals with mobile telecommunication

---

14 Online panel survey of 1 500 persons in May 2002.

15 In addition, from an economic point of view, mobile commerce can also offer consumers some of the same benefits as the Internet: *i)* lower prices due to price comparisons and information about how to negotiate with dealers (*e.g.* Brown and Goolsbee, 2002; Zettelmeyer *et al*., 2004); *ii)* greater choice, increased demand as a result of competition (*e.g.* competition between online dealers and between bricks-and-mortar and online dealers) and improved consumer welfare (*e.g.* Gu *et al*., 2004); *iii)* improvement of asymmetric information [*e.g.* health services (Masi *et al*., 2003); air travel (McAfee and Hendricks, 2003); financial investment (Lin and Lee, 2004; Lee and Cho, 2005); health care services (Snies *et al*., 2005); reputation system (Resnick and Zeckhauser, 2002)].

16 According to the Cabinet Office (2006), 26.4% of parents did not wish their children to have mobile phones.

17 "Handy lost Auto als Schuldenfalle ab!" in September 2005 by Market Group (in German).

issues. The Working Party on the Information Economy (WPIE), in particular, has a large stream of work on digital content, including mobile content.[18]

This report presents an overview of the market and policy frameworks for mobile commerce in OECD member countries with the objective of sharing experience and helping policy makers to examine their current policies. Part I focuses on business trends and the development of market services. Part II describes some technological solutions for market development. Part III describes consumer policy measures adopted by government and businesses to give consumers confidence in the market. Part IV touches on security and privacy concerns. A brief conclusion follows.

[18] See all WPIE work and publications, such as OECD (2005c, 2005d, 2005e; 2006), on www.oecd.org/sti/digitalcontent; and Annex D. The OECD Information Technology outlook 2006 also has a section of mobile content in page 191.

I. BUSINESS TRENDS AND DEVELOPMENT OF MOBILE SERVICES

How large is the current mobile commerce market (domestic use only?)

It is difficult to estimate the mobile commerce market across countries because of differences in definitions. However, the available data provide an initial indication of the current and potential future market.[19]

Individuals, particularly in Japan and Korea, have started to own the Internet-connectable mobile phones that enable the development of mobile commerce (Figure 1). In a press release of 18 July 2006, the Foundation for Multi-Media Communications and Mobile Content Forum estimated the mobile content industry market in Japan at around JPY 722.4 billion (around USD 6.12 billion) in 2005. Consumers bought mobile content such as music for about JPY 315.0 billion (around USD 2.67 billion), an increase of 21% over the previous year. They also bought goods or services via mobile phones for around JPY 407.4 billion (around USD 3.45 billion), an increase of 57% over the previous year. In Korea, the mobile Internet market was projected to be worth KRW 3.08 trillion (around USD 2.6 billion) in 2004 (OECD, 2004b).[20] The European market for mobile content in 2002, as estimated by Andersen (European Commission, 2002), was around EUR 2 billion (around USD 2.45 billion) and was projected to range between EUR 7.8 billion and EUR 27.4 billion in 2006, with a median forecast of EUR 18.9 billion (around USD 23.2 billion).[21] The Latin American market[22] was around USD 592 million in 2005, an increase of 120.5% over the previous year (Frost and Sullivan, 2006).

However, this is a very small share of the whole domestic market and it is also a good deal smaller than fixed computer-based e-commerce. For example, in Europe, the mobile commerce market may be only around 20% of the business-to-consumer (B2C) e-commerce market in 2006.[23] Even in Korea, the mobile commerce market consisted of only around 48.1% of the B2C e-commerce market in 2004.[24] In Japan, it represented only about 17.2% of that B2C e-commerce market in that year (MIC, 2006, p. 65). Micro data confirm that even though most mobile phone subscribers can connect to the Internet, only 2.1-7.9% used a mobile phone for mobile commerce once a month in 2004 and spent an average of

---

19 For the technological and business developments on mobile content, see OECD (2005c) and Annex D.

20 According to the Federation of Korean Information Industries, wireless data service revenues in 2005 were KRW 3.4 trillion (USD 3.57 billion) and were expected to grow by 11.8% to KRW 3.8 trillion (USD 3.99 billion) in 2006.

21 Other data sources put the mobile content services market in Norway at around NOK 800 million in 2004 (around EUR 90 million and USD 117 million) and NOK 1 billion in 2005 (around EUR 125 million and USD 150 million). In the United States, data for market size of mobile commerce alone are not available, but household expenditures for mobile telephone services, including voice, increased 892% from 1995 to 2002.

22 Argentina, Brazil, Chile, Colombia, Mexico and Venezuela; 46.4 million people used mobile content services in 2005, or 26% of the total number of mobile subscribers.

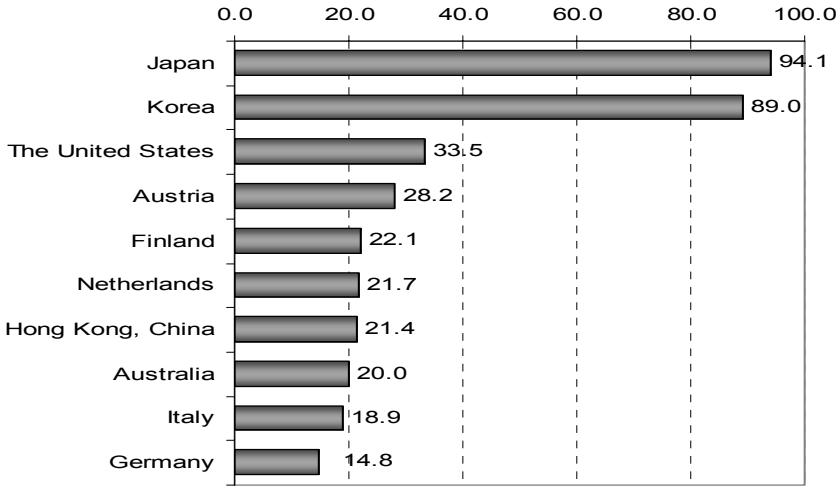
23 eMarketer (2006) estimates that total retail e-commerce sales in Western Europe will reach USD 96.6 billion in 2006. It is only accumulated figures of 5 countries include the United Kingdom, Germany, France, Italy and Spain.

24 Although the difference of data sources and definitions may be difficult to compare two figures (*e.g.* exclusion of C2C), the Korea National Statistical Office reported a B2C e-commerce market of around KRW 6.4 trillion in 2004 (KNSO, 2005) and around KRW 7.9 trillion in 2005 (KNSO, 2006).

JPY 4 921 (USD 46); in contrast 53.0% use computers for e-commerce and spend an average of JPY 9 652 (USD 90) (Mitsubishi Research Institute and Rakuten, Inc., 2005a).

A survey by the Electronic Commerce Promotion Council of Japan (ECOM, 2004b) shows that consumers in Japan, Korea, Chinese Taipei and Greece are more interested in mobile communications, such as SMS, than in mobile commerce.[25] Also, the global mobile data research study, known as the "Mobinet Index", by A.T. Kearney and Judge Institute of Management, University of Cambridge (2005), shows that 57% of mobile users are not willing to pay more than USD 5 a month for mobile data services (the researchers' definition of mobile data services includes both text and photo messages).[26]

Figure 1. **Internet-connectable devices as a share of total mobile phone subscribers in selected countries**
September 2004



Note: Figures are calculated from subscribers to the main carriers in each country.
Source: MIC (2005), *Information and Telecommunication in Japan 2005*, Figure 5, page 86.

With regard to mobile commerce payment methods, the Cabinet Office of Japan (2006) indicates that adding fees to mobile telephone bills is the most popular method (46.6%), followed by money transfer (17.6%) and credit card payment (11.3%). In other countries, use of credit cards for payment may be much higher.

How big will the market be in the near future?

Research companies see mobile commerce developing significantly. Juniper Research (2004) estimated that global revenues would represent around USD 88 billion in 2009. iGillott Research (2005) predicted that non-SMS wireless data and media services would be around USD 80 billion by 2009. The Yankee Group (2005) forecast that mobile data services in 2009 would reach around USD 146 billion, more than 21% of worldwide wireless operator service revenue. Portio Research (2006a) predicted that the

25 Mahatanankoon *et al.* (2005) shows that the US consumers (university students) prefer sending or receiving e-mails to receiving time-sensitive information (*e.g.* weather reports and traffic information) or downloading MP3 songs.

26 The survey has been done every year for the past eight years. The latest, released in October 2005, is based on interviews of 4 000 mobile users in 21 countries: Australia, Brazil, Canada, China, the Czech Republic, Denmark, Finland, France, Germany, Japan, Italy, Korea, Mexico, New Zealand, Poland, Portugal, Russia, Spain, Sweden, the United Kingdom and the United States.

mobile content market would more than triple to USD 59 billion over the four years to 2009 because of great developments in gambling and online games. Registrations under a new domain name for mobile (.mobi) started in October 2006 and may boost mobile commerce.[27]

In Finland, one of the most developed mobile services market, content and data services are expected to grow by 40% over the coming two years from EUR 88 million in 2004 to EUR 124 million in 2006 (Ministry of Transport and Communications, 2005, p. 26), although person-to-person e-mail is still the industry's largest source of revenue. A survey by Portio Research (2006b) mentions that Spain, Italy and Poland will be the hottest European mobile multimedia content markets in the coming years. In Korea, the market is expected to more than double in value within six years.[28] In Australia, the mobile content market is expected to increase 7.9 times more from AUD 129 million (around USD 96 million) in 2004 to AUD 1.015 billion (around USD 756 million) in 2009 (Australian Communications and Media Authority, 2005, p. 89). Frost and Sullivan (2006) predict that mobile content services in Latin American markets will grow by a factor of 4.4 and reach USD 2.61 billion in 2012.

The Mobinet Index (A.T. Kearney and University of Cambridge, 2005) classified 40% of mobile users as emerging users of data services (those who agree or strongly agree that they are willing to use a mobile phone as a data services device). For example, in Japan they represent 71% of mobile users, in Australia and New Zealand 53%, in China and Korea 43%, and in Scandinavia and Western Europe 41%.

No data are available on current cross-border mobile commerce, but cross-border use of mobile commerce has huge potential. In Japan, for instance, 24% of those who had travelled abroad during the year wished to use mobile phones abroad to find information such as traffic, weather and tourist sites on the web during their next trip (NTT DoCoMo, 2005, Figure 5). More than 30% of males in their teens and 30s expressed this wish.

What kind of goods and services do consumers buy via a mobile?

According to ECOM (2004b), downloading music for ringtones represented the largest share of mobile commerce (Table 3).[29] This is confirmed by other data sources, although the downloading of music has decreased in Japan (Table 4). The results are similar for the EU (EC, 2002). Mobile commerce is currently most popular for games, music and news (OECD, 2005c, indicates that music and games are viewed as a major emerging industry).

According to a survey by the Australian Interactive Media Industry Association (AIMIA, 2006), 66% of Australian consumers purchased mobile content and 59% accessed information services in the previous 12 months although purchases were infrequent. The dominant services are ringtones (nearly half), wallpaper (23%) and news (22%); those in the 13-16 and 19-25 age groups purchased more content than those in other age groups. In the United States, although a survey by the Pew Internet & American Life Project (2006a) suggests that mobile phones are still essentially voice call devices, consumers are also using them to play games (22%), access the Internet (14%), perform Internet searches (7%), get maps (4%), and watch video or TV programmes (2%), especially in the age group 18-29 (47%, 28%, 17%, 9%

27 See http://pc.mtld.mobi/. The registering organisation expects to register 200 000 sites within a year. dotMobi has also issued best practice guides for developing mobile content and services.

28 Figures from a survey by IBSNet, cited by Dr. Jong-In Lee of the Korean Consumer Protection Board at the OECD CCP forum session on mobile commerce in March 2005. The size of the market is expected to increase from KRW 3.08 trillion in 2004 to KRW 6.839 trillion in 2010.

29 According to the 2006 Korea Internet White Paper (NIDA, 2006, pp. 61-62), most users had downloaded ringtones (96.8%), followed by streaming and downloading music (45.4%), downloading and transferring photos and video (42.1%) and online gaming (37.1%).

and 5% respectively). Among respondents whose mobile devices did not have these functions, 47% said they would use them to get maps and 24% to perform Internet searches.

Table 3. **Most frequent use of mobile commerce in selected countries**

	Japan	Korea	Hong Kong, China	Chinese Taipei	Greece	Finland
Sample (persons)	2 146	4 581	1 375	1 809	497	66
First place	Download services (28.8%)	Download services (60.0%)	Reading (58.0%)	Download services (36.1%)	News (12.1%)	Download services (31.8%)
Second place	News (16.2%)	Games (17.2%)	Deliver Services (21.6%)	News (14.1%)	Download services (9.9%)	News (24.2%)
Third place	Location Information (14.9%)	Ticketing for movie/music (12.7%)	Games (16.9%)	Investment info/trans (10.2%)	Weather report (9.1%)	Financial services (9.1%)

Source: Based on ECOM (2004b) *Survey of Mobile Internet Use*, Tables 3-5 and 3-7.

Table 4. **i-mode menu sites consulted, % of total**

	FY2001	FY2004	FY2005
Music for ringtones and screen savers	42	30	21
Games and horoscope	19	22	24
Other entertainment or Information	19	24	27
Information	10	12	12
Database	5	4	5
Transactions	5	8	11

Source: NTT DoCoMo, Operating Data for Investor Relations.

What kinds of new services are emerging?

No single dominant value chain has emerged and it is likely that different value chains will prevail for different types of mobile content, reflecting market structures. Numerous market players, content owners and developers, content aggregators, mobile operators, handset manufacturers and various other businesses are entering the market and are competing (see OECD, 2005c). In this market situation, many new services are being offered. In addition to ringtones, music, games, news and other information services, financial services, location-based services, mobile television, subscription radio and online comic books (*Manga*) are entering the mobile commerce market.

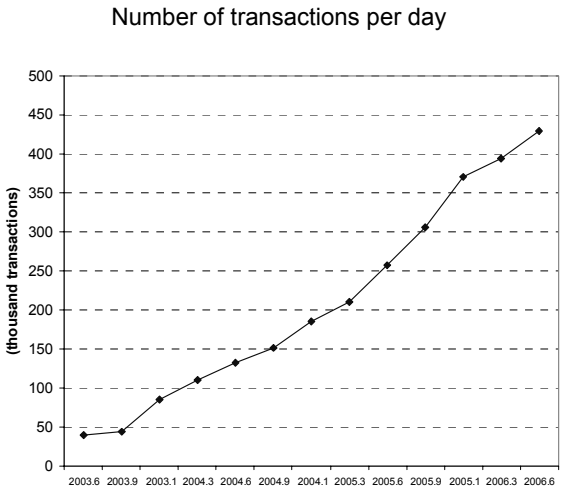
Integrated financial services are a prominent service. In Korea, SK Telecom has introduced MONETA, a wired and wireless integrated financial services via mobile phones.[30] To use these services, an individual must become a member of the wire-line MONETA service, and obtain wired and wireless service authentication from SK Telecom. The MONETA card allows customers to make mobile payments by inserting their MONETA chip into their mobile phones. It serves as a credit card, a membership card, a ticket and a discount coupon. It can be used as a credit card by entering the password for the card on the individual's own terminal. It is said that the MONETA card's IC chip cannot be falsified or reproduced. MONETA also offers money transfer services, so-called "MONETA cash", which makes it possible to

30 Mr. Jae Kim of SK Telecom explained the service at the CCP forum in March 2005.

transfer money to the recipient's phone number. The recipient's name, the bank's name and account number are not necessary. A message can accompany the transaction and a confirmation message indicates when the transmission has succeeded. Payments can also be made to other MONETA cash subscribers.

In Korea, *mobile banking* is also widespread. In September 2003, LG Telecom and Kookmin Bank started "Bank On" services, in which a mobile IC chip is used to make one-click online transactions in real time. This easy-to-use and rapid function gained them new customers. SK Telecom and KTF, other two Korean telecom carriers, started similar services in March 2004 and the number of transactions has increased steadily. Around 2.4 million consumers have registered with these mobile services, and, according to the Bank of Korea, around 430 000 transactions a day were handled in June 2006, an increase of 67.3% from the previous year (Figure 2).

Figure 2**. Mobile banking in Korea**



Source: Bank of Korea (2004, 2005, 2006b).

In Japan, with cooperation from JCB, a credit card company, Au by KDDI, a mobile carrier, is going to pre-install software in the IC chips in most of their mobile devices so that they can be used as a credit card. NTT DoCoMo started a new service, called i-mode Felica, in July 2004.[31] All three mobile carriers in Japan have now introduced "Osaifu Keitai" (mobile wallet) with contactless cards like those of Suica, Edy, Smart Plus, QUICPay and Visa Touch.[32] Like MONETA in Korea, the contactless cards make it possible to use a mobile for electronic money, membership card, tickets and electronic keys. In Finland, mobile-based banking services have been available since 1996. In addition to the services by banks (*e.g*. EMPS by Nordea Bank), non-bank firms now provide financial services such as "DNX MobileMoney", "Sonera Shopper" and "E-Pay" (Jyrkönen and Paunonen, 2003). In Belgium, Banksys, a credit card company, in conjunction with three major mobile carriers, plans to start its "m-banxafe" service through SIM cards by the end of 2006. When a consumer receives a text message from Banksys, he/she can authorise payment by his/her bank by a special personal identification number (PIN) code. Mobister, the second largest mobile

31 Mr. Seishi Tsukada from NTT DoCoMo Europe (France) explained the services at the CCP forum in March 2005.

32 According to MRI and Rakuten (2006), consumers make little use of these functions. Only 3.1% of individuals overall used these functions although males in their 40s and 30s use it more (9.4% and 7.0%, respectively). In addition, those in their teens also expect to use these function although the current usage rate is low (3.0% for males and 0.5% for females). Visa International announced that it would introduce "Visa Touch" contactless IC card services (press release of 12 June 2006).

carrier in Belgium, has already put the application software on all of its new SIM cards (Banksys, 2005, p. 18). In the United States, a virtual payment solution company, Vesta, announced on 1 February 2006 a SIM-based mobile payment scheme for prepaid mobile phones subscribers with Axalto, a smartcard company. [33]

Many of the early *location-based services* were "one-off" services provided at the user's request, such as information on the nearest restaurant or petrol station to the user's position. Now, using the Global Positioning Systems (GPS) technology, location-based information services are more widely available. In Japan, for example, Au by KDDI offers navigation services that provide an on-screen map and voice-over navigation instructions. Vodafone Japan provides the similar services. Also, NTT DoCoMo has started "imadoco search" services, which enable a parent to know where a child is located through a mobile or computer screen.[34] In Korea, LG Telecom introduced an auto navigation service in September 2004. KT telecom provides "i-Kids" service including GPS tracking to show a child's location. In the United States, for instance, a free service, "Mologogo", will track a friend's GPS-enabled mobile phone from another phone or website with a subscription (www.mologogo.com). In fact, US consumers consider GPS the most desirable feature on a mobile phone (50%) above Bluetooth (30%), e-mail (29%), broadband Internet (26%), and MP3 (23%) if they do not already have these functions (Rockbridge Associates and Robert H. Smith School of Business at the University of Maryland, 2006).

Mobile *digital TV services* have been launched or tested in many member countries. In Korea, a satellite mobile broadcasting (DMB) company, Tu Media, announced on 2 May 2006 that their mobile service subscribers reached 540 000 in April 2006 since they started the services in May 2005 and that 63% of their subscribers are in their 20s and 30s.[35] German and Italian mobile carriers launched mobile television services in May 2006. In Japan, "one-seg" (one-segment) broadcasting services were launched in April 2006, and JEITA (Japan Electronics and Information Technology Industries Association) announced in August that more than 1.18 million mobile devices with a "one-seg" TV tuner had been sold by June 2006.[36] Other countries have begun trials of mobile digital TV. For instance, in Sweden, Telia Sonera Sweden launched a test in Stockholm in August 2006.[37] In Finland, the United Kingdom and the United States, services will start during the second half of 2006. Juniper Research (2006a) forecasts that mobile digital TV services will grow from USD 94.57 million in 2006 to USD 11.7 billion around 2008-09.

Among the other kinds of mobile commerce services that have been launched, mPARK (mobile payment parking system) makes it possible to pay parking fees with a mobile phone in Edinburgh, Scotland, Cologne, Germany, and Oklahoma City, United States. In Norway, Telenor has launched the "MobilHandle", which allows subscribers to buy DVDs, music CDs, concert and cinema tickets and ski lift tickets. One can also bid on a horserace by using a loaded smart cash or Visa card. The 500 000 subscribers represent 22% of Telenor's mobile phone subscribers. In Finland, consumers can buy products from 800 vending machines by calling a premium rate number.

The city of London implemented a traffic congestion charge in February 2003. As well as paying on line, at selected shops, petrol stations and car parks, by fixed-line telephone or by post, motorists can also pay their charge by mobile phone using an SMS text message. This service requires them to register, and

---

33 According to a survey by In-Stat (2006), 10 to 25 million mobile subscribers in North America could be using mobile wallet by 2011.

34 This service is offered because many children are victims of criminals these days. Even if the child's mobile phone is switched off, GPS estimates the child's location. See also Mahatanonkoon *et al*. (2005).

35 The press release is only available in Hangul.

36 The press release of 25 August 2006 is only available in Japanese.

37 Press release of 19 June 2006.

when their information is verified by the exchange of a secure token sent as a text message back to their phone, they can pay the charge with a simple SMS text message from their registered phone. To pay the charge for that day, they simply send a text message to the fixed number with the last four digits of their credit or debit card. They then receive a confirmation message on the mobile phone acknowledging payment for the vehicle they have registered. A doctor consultation service through 3G mobile phones will be launched in the United Kingdom by the end of 2006 (www.3gdoctor.com).

In an international context, Jorudan, a Japanese mobile service provider, launched in December 2003 services to provide Japanese tourists abroad with transport maps, metro transfer information, and information on tourist sites in New York, Paris and London (press releases of 14 November 2003 and 7 February 2005). Another project aims to allow any mobile device in the world to connect to Japanese information sites.

II. TECHNOLOGICAL DEVELOPMENT

What technologies affect the development of mobile commerce?

The technologies necessary to enable broad dissemination of content, including marketing, distribution and billing, are increasingly available and will encourage further development of mobile content.[38] Technological developments also provide some protection against the disadvantages of mobile commerce. As noted, the main consumer concerns are the small screen, limited availability of information and security. This section takes a look at technologies to address these issues: browsers, memory size, content delivery system, payment scheme, bar code readers and Mobile WiMAX.[39]

Full browsing function

Some software companies are developing software that allows mobile users to look at Internet sites on small mobile screens more easily (*e.g.* Opera Mobile™, Scope, jig browser, Site Sneaker, Glupo). Some mobile carriers preinstall such software and some software can be downloaded directly to mobile phones. Users can use the software to show several pages simultaneously and look at web pages with large amounts of data such as maps.[40]

The appearance of web pages depends on the software architecture: for example, how it presents the pages on a small screen, whether it allows certification to identify users, whether it allows use of javascript, and whether or not the font is easy to read. Furthermore, all mobile devices cannot install all software. There is currently no software available that can resolve all of these issues.[41]

Memory size

Mobile phones with large amounts of memory can be used to transfer content with large data requirements such as music, games and videos. In addition, large storage may allow installing the filtering software, which is usually required large memory, at some time in the future. For example, at Telecom Asia 2004, Pantech & Curitel, a Korean company, issued a phone with 1 Gigabyte of memory. At the 3 GSM World Congress in 2006, Nokia issued a phone with 4 Gigabyte hard disk drive (HDD), and Sony

---

38 Annex B lists organisations that promote mobile commerce in industries. See also OECD (2005c), Section 2.

39 System architecture also plays a role in consumer issues. For instance, it can deal with problems of temporary unavailability (*i.e.* link outages) by integrating web service technology into wireless services such as message queuing and WWW wireless optimisation mechanisms. See Piloura *et al.* (2005) and Kumar *et al.* (2005).

40 AlShaali and Varshney (2005) note that even when greater amounts of information are available on the Internet, most users are unable to find the desired information; thus, mobile commerce depends more on how information is organised and browsed than on the appearance of web pages.

41 MRI and Rakuten (2005b) indicate that 40% of users expressed willingness to use the software when they assess to the internet. However, they raised issues such as the high cost of connecting to data services (60.8%), the small screen size (44.3%), difficulty for reading because of poor layout (28.1%), and scarcity of applicable devices (25.9%).

Ericsson issued a phone with a 4 Gigabyte memory card. In March 2006, Samsung announced that it would introduce a phone with an 8 Gigabyte HDD in the second half of 2006. Competition to put more memory on mobile phones will continue.

Content delivery system

To find ways to secure safe and controlled use of mobile content services, carriers and mobile device manufacturers are testing a variety of initiatives: a log-in membership system, a PIN number requirement, age certification, and a blocking and filtering system. In the United Kingdom, all networks offered the last of these mechanisms in January 2004. A number of content providers have been suspended by the operators because they do not comply with a "Code of Practice on Content".

In Finland, Nokia has launched a new service based on subscriber and mobile service recognition. It allows mobile users to control access to mobile content services, *e.g.* parents can prevent children from accessing undesirable or unwanted services (press release of 22 September 2004). In Germany, some mobile carriers offer prepaid cards tailored to minors which do not give them access to certain expensive premium rate services.

In Korea, KT Telecom has begun a service which allows parents to cut off a child's access to Internet services if a mobile phone is subscribed by a name of a child under the age of 18. The service allows parents to block not only adult content but also other mobile Internet services such as music downloading, online games and banking services which are provided under the name of "June" and "Nate". In addition, in June 2006 KT Telecom introduced a data usage fee notification service. With this service, parents set a ceiling of between KRW 20 000 (around USD 21) and KRW 150 000 (around USD 158) and when the child's usage reaches the prescribed ceiling, only the parents can restart the service.[42]

Payment systems

There are three main payment options. First, when users buy something via their mobile phone their service carriers can add the charge to the mobile phone bill. Second, a contactless (or "proximity" and "vicinity") IC card is a potential payment tool.[43] With a mobile phone with a contactless IC card, it is easy to recharge and authenticate the prepaid function through the telecommunications system. Third, credit card information can be read on mobile phones using infrared ray technology. IrDA is the technology standard. Businesses are examining the architecture or business model for mobile payment in organisations such as Mobey Forum and Mobile Payment Forum (see Annex B). Authentication is a key development area for mobile payment.

---

42 Press release of 5 June 2006. See: http://www.sktelecom.com/kor/cyberpr/press/1197909_3261.html (in Hangul)

43 The contactless IC card is generally based on ISO14443, which uses 13.56 MHz. If the card is placed within 10 centimetres of an IC reader, the machine can read the data on the card.

ISO standard for contactless IC card

ISO standard	Category	Frequency range	Maximum distance	Usage
ISO14443	Type A	13.56MHz	10 cm	Card, Mifare (Philips)
	Type B	13.56		CARD, SD CARD (VODAFONE)
	Type C	13.56		ELECTRIC MONEY, PREPAID CARD, FELICA (SONY)
ISO15693		13.56	70 cm	Tag/card

Source: IT Media News, "Mobile+ Contactless IC = ?", September 18th, 2002 and others.

On the other hand, hacked, lost or stolen mobile devices may cause leakage of confidential and/or privacy information, especially payment information. Prevention measures used include wireless authentication and encryption. For instance, in Korea, SK Telecom provides wireless authentication services, "MONETA Sign", and mobile online signature free of charge to subscribers.[44] LG Telecom uses triple-DES (a data encryption standard) for their Bank-On service. Other companies have started to provide biometric authentication by face and fingerprint recognition (*e.g.* NTT DoCoMo).

Some mobile operators provide on-demand remote access to lock down (or wipe clean) a device to prevent unauthorised use of mobile devices if they are stolen.[45] For instance, SOFTBANK MOBILE Corp. (formerly Vodafone Japan) has provided remote lock services by calls and e-mail for mobile phones with contactless cards since November 2005; if a user sets the function as calling five times from his/her home telephone within 3 minutes, this locks the IC tip if she exactly does so.[46]

Cryptographic functions such as SSL (Secure Sockets Layer) and WTLS (Transport Layer Security) are now widely available over mobile screens. Public key infrastructure (PKI) can also be housed in a mobile IC chip. In 2005, E-Bank, a Japanese online bank, started to offer services to allow their customers with mobile PKI functions to access their accounts and to lock or unlock their device or to withdraw funds from an automatic teller machine (ATM) at a bank branch.[47] However, it is said that current PKI technology uses a lot of time and energy with mobile devices because of the limited bit size of the CPU (central processing unit).[48]

Bar (or two-dimensional) code reader

Many mobile devices now have a barcode reader function[49] which allows consumers to reach a website easily by holding their mobile phone up to a code. The installed software then calls up the relevant site.[50] For example, if a consumer holds a mobile device over an apple in the supermarket, he/she can

---

44 See more their website: sign.moneta.co.kr (Hangul only).

45 Even though there are already some security functions and users recognise them, they do not often use them. According to Nikkei BP (2005), even among business persons, only 5.5% set remote lock and 1.8% set remote wipe-clean function. The preferred function is PIN code protection, which is used by 33.7%.

46 Users in Japan cannot be protected from unauthorised use of prepaid card function because of no legal protection. Also, the lock does not function when the mobile phone is switched off or out of the service area.

47 In Japan, mobile carriers have PKI services, with a registration fee, mainly for business customers (*e.g.* Security Pass at Au by KDDI and First Pass at NTT DoCoMo).

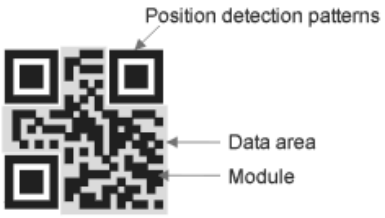
48 To improve processing speed, mobile device manufacturers have started to use twin CPUs to separate communication and application processing.

49 In Japan, QR Codes, which are 2-dimensional UPC or barcodes, are common. They hold much more data than a traditional barcode. They include all types of data, such as numeric and alphabetic characters, Kanji, Kana, Hiragana, symbols, binary and control codes. Up to 7 089 characters can be encoded in one symbol. The QR Code was approved as an ISO international standard (ISO/IEC18004) in 2000. It can be read by a visual scanner.

50 Laboratory experiments show that information received through mobile handsets can help improve consumer decision making even if more alternative products are offered to consumers (Heiden, 2005).

identify the farmer who produced it. In Japan, these codes are widespread, not only in products in stores but also in journals and on posters.[51]

Figure 3: **A Sample of QR code**



Note: The image is from Daiso Wave Cooperation.

Mobile WiMAX[52]

WiMAX[53] is a standards-based technology which allows for the delivery of last-mile wireless broadband access without the need for direct line-of-sight to a base station. WiMAX provides fixed, nomadic, portable and, ultimately, mobile wireless broadband connectivity. This means that consumers will be able to transfer the connection seamlessly between mobile and fixed devices. In Korea, KT launched "KT WiBro" services around Seoul in June 2006;[54] SK Telecom launched the same kind of services in the same month. A report predicts that WiBro subscribers in Korea will reach around 2 million in 2007 and 7 million in 2011 (ATLAS Research Group and Info-Sharing Business Institute, 2006). Cetecom Spain started to test the product at its official certification laboratory in July 2005. In the United States, Sprint announced on 8 August 2006 that WiMAX-based broadband services (4G) will be tested by the end of 2007. Commercialisation of this technology has just begun, but it may make it possible to transfer mobile transactions to stationary computer terminals.

---

51 Scornavacca and Barnes (2006) examine three cases of barcode enabled m-commerce. According to MCI and Rakuten (2005a), the most popular users of this function in Japan are men in their teens (45.3%) and 20s (41.0%) and women in their 20s (40.0%).

52 See also OECD (2005b). In addition, Working Party on Communication Infrastructures and Services Policy (CISP) under ICCP is currently discussing about policy issues of fixed-mobile convergence.

53 Working Group 802.16 in the Institute for Electrical and Electronics Engineers (IEEE) standardised the WiMAX.

54 Press release of 29 June 2006 (in Hangul). WiBro (Wireless Broadband), the technology that is being developed in Korea, is recognised as one type of WiMax. KT already has a "Nespot Swing" service which provides continuous data coverage as a subscriber moves between KT's Wi-Fi network "Nespot" and the CDMA2000 1x EV-DO network of KT's sister mobile network, KTF.

III. CONSUMER PROTECTION CONCERNS

Mobile commerce raises a number of important consumer policy issues, especially regarding unsolicited sales, inadequate information disclosure and protection of minors.[55] Unauthorised use and SMS spam are also issues. While the technological developments described above can address some aspects of these issues, legal protection, self-regulation by business and consumer information campaigns are essential.[56] This section looks at the measures that have been put in place to date to address consumer concerns relating to mobile commerce.[57]

What kinds of consumer complaints have member countries received?

A survey in Japan asked consumers whether they had any concerns about mobile payment schemes (MRI and Rakuten, 2004). Respondents named privacy issues (78.2%) and the potential increase in misuse and theft (75.9%) as the biggest source of concern. A survey of its members by Consumers International indicated that they were very or fairly concerned about the following issues: adequacy of disclosure about the product or services offered and about the total cost; liability for charges made by others without the knowledge or consent of the phone customer; adequacy of disclosure about terms and conditions for subscription services; security of payment transactions over mobile handsets; privacy of data when the phone is lost or stolen; and targeting of minors through aggressive marketing practices.[58] Another survey conducted by the Trans Atlantic Consumer Dialogue (TACD), a coalition of consumer organisations in the United States and the European Union, revealed that consumers have major concerns about mobile commerce, especially with regard to the adequacy of information about the product or service offered, the terms of sale, and the total cost; spam; data protection and security; and redress mechanisms (TACD, 2006).[59]

In terms of consumer complaints, some member countries have never yet officially received consumer complaints concerning mobile commerce (*e.g.* the Czech Republic, Canada, France, Mexico, Poland and the Slovak Republic). However, the number of complaints is increasing dramatically in some countries. In Norway in 2005, based on high numbers of consumer complaints, the Consumer Ombudsman handled 115

---

55 This section is mainly based on responses to the questionnaire on consumer policy issues associated with mobile commerce (DSTI/CP(2005)14) which aimed to assess the mechanisms and initiatives used to address these issues. By September 2006, 19 member countries and the European Commission had responded (see also Annex C). Because this project did not cover issues relating to voice call pricing and messaging tariffs by mobile carriers, these are not discussed here.

56 Ms. Claire Alexandre of Vodafone stated at the CCP forum that to restore confidence, technology is only a last resort. Technology developments can improve transparency, but abusers always run ahead of them.

57 According to Ngai and Gunasekaran (2005), only a few articles explore the legal and ethical issues associated with mobile commerce. Also, see Rawson (2002).

58 Reported by Ms. Anna Fielder, former Director, Consumers International, at the forum session on mobile commerce during the 69th session of CCP in March 2005.

59 TACD (2006) revealed that 38% of respondents had experienced problems related to mobile commerce within the last 12 months. It also showed that the extent of consumer problems may not be fully reflected in government complaint statistics, as 59% of the survey respondents who had problems never reported them to anyone, and only 12% contacted government agencies.

consumer cases relating to mobile content service issues and 60 cases concerning unsolicited advertising via SMS.

At present, consumer complaints in OECD member countries typically fall into three categories: *i)* unsolicited sales of content or services; *ii)* inadequate information disclosure; and *iii)* issues relating to minors such as inappropriate marketing and over-consumption.

In terms of unsolicited sales, Swiss consumers have received and been charged for logos, ringtones and premium services which they allegedly had not ordered. In Sweden, when consumers accepted an offer of free ringtones or similar content by replying to a message, they later received content weekly and were subsequently billed for it. Finland has had similar problems. Also, the Norwegian and the Finnish Consumer Ombudsmen received many complaints about insufficient information about the pricing of mobile content services and the difficulty of checking costs. The National Consumer Affairs Center of Japan (NCAC) has received many similar complaints. For example, a student 17 years old accessed a "free" adult photo site he had heard about from a friend but found the following message: "Please pay JPY 50 000 (around USD 430) as the usage fee for our site within 3 days". When he made a call to the site operator, there was only a recorded voice presenting the adult-oriented programme. He then received another message from the operator: "If you ignore the bill, forcible recovery of the claim shall be carried out."

For inadequate information disclosure, owing in part to limitations on the memory and screen size of mobile devices, consumers in some member countries may simply be presented with "click-wrap" agreements and may not have access to, or be provided with, a full version of the contract, comprehensive terms and conditions or details of complaint handling mechanisms before entering into an agreement. The Norwegian Consumer Ombudsman also received many complaints about insufficient information about the pricing of mobile content services and the difficulty of checking costs. The TACD survey (TACD, 2006) also indicated that the most frequently cited problem relating to mobile commerce was that the cost of goods or services was inaccurate or misleading (35%).

Regarding payment liability issues, many consumers in Finland were imposed liability by companies offering instant loan even though they did not take out a loan. It happened because a person can take out an instant loan with a text message in another person's name by using the person's mobile phone number and ID number but the company did not check the identity of the sender.[60]

Regarding minors, the Finnish Consumer Ombudsman, for example, has received numerous reports from parents who have had to pay hundreds of euros in mobile phone bills because their children have participated in interactive TV games and chat programmes by sending text messages. The Danish Consumer Ombudsman has received similar complaints.

Other complaints concern non-delivery of the mobile content ordered, opaque and/or unfair complaint mechanisms, insecure mobile payment transactions and other technical drawbacks of mobile telecommunication networks, and privacy concerns. Spam to mobile devices is also a big concern.[61]

---

60 The instant loan services initially appeared a problem about marketing as the fact that there were not any contract terms which consumers can cancel a loan. Then, it caused another problem that those companies did not display enough information and contract even though they can use text messages to do so. See more: uutiskirje.kuluttajavirasto.fi/consumer_law/consumer_law_4_2006/en_GB/instant_loans/

61 According to Rettie *et al.* (2005), SMS advertising is much more effective than direct mail and Internet e-mail marketing, with an average response rate of 31% for 26 campaigns. As a result, using location information, push advertising allow businesses to advertise to individuals nearby via their mobile phones. See, for instance: www.yellowmap.com/english/lba.asp; www.blueblitz.com; www.toroblue.com; and

Complaints related to cross-border cases have become more common in member countries. For example, Finnish consumers have received fraudulent "free" offers for ringtones from a business located in another country. Other serious cases have involved stolen devices in Japan (NCAC, 2006). For example, a Japanese woman took her mobile phone abroad to use it as a digital camera and it was stolen. She reported the theft to the local police but did not report it immediately to her mobile phone company because the mobile company's brochure stated that the phone was for domestic use only and her understanding was that it could not be used abroad. However, she was later charged around JPY 3 million (around USD 25 600) because her IC card was removed from her device and inserted into another device that could be used abroad. With integrated payment systems, mobile phones are becoming one-stop platforms and can also function as cross-over platforms with electric money, prepaid money, credit card, telephone bills, etc. Depending on the function or business, protection measures may differ and risks to be stolen and misused are greatly increased.[62]

Theft of mobile phones is in fact a worldwide issue because of the economic motivation to steal personal and financial data. As mentioned earlier, the potential increase of misuse and theft is one of the biggest concerns of mobile users. In fact, more than half of the 4 000 street crimes in London every month involve the theft of a mobile phone and in 1 200 cases the victims' handsets are specifically targeted (Juniper Research, 2006b). In the United Kingdom, 10 000 mobile phones are reported stolen every month. Juniper Research (2006b) also predicts that number of mobile phone stolen will more than double in Asia-Pacific and will double in the North America during the next five years. Thus, cross-border protection for unauthorised use will be a significant issue.

Protection for mobile commerce transactions

Countries with well-developed mobile commerce markets face problems such as unsolicited sales and non-delivery of the mobile content ordered. Most of these countries are tackling these problems with general consumer protection acts (*e.g.* fair trade acts, consumer protection acts) or distance sales acts, including acts on electronic commerce in addition to self-regulation.

What kinds of protection schemes for mobile commerce transactions do member countries have?

Some countries apply general provisions prohibiting unfair or deceptive acts or practices to consumer protection issues relating to mobile commerce. For example, the provision prohibiting misleading representations and deceptive marketing practices in Canada's Competition Act is technologically neutral. Similarly, the Australian Trade Practices Act is technologically neutral with provisions that apply equally to mobile commerce issues and non-mobile forms of trading. Also, in the United States, the Federal Trade Commission Act (FTC Act), which prohibits "unfair or deceptive acts or practices in or affecting commerce" would apply to mobile commerce. Germany and Switzerland report that they apply consumer contract provisions to mobile commerce. In addition to the general consumer protection provision, countries such as Austria, Belgium, the Czech Republic, Japan, Korea, Mexico, Poland, the Slovak Republic, Sweden and the United Kingdom report that they apply distance sales regulations, and more specifically regulations on electronic commerce. [63] The European Commission also reports that the

---

www.ad2hand.com. More sophisticated forms of mobile advertising using multimedia such as video and digital TV are also being tested in the market.

62 An earlier report on payment cards already noted that "An issue for future examination is how these legal and regulatory regimes will apply to other payment systems once they come into more widespread use by consumers, especially in their online purchases" (OECD, 2001, p. 15).

63 In the case of Mexico, the Federal Law of Consumer Protection (LFPC) regulates all kinds of commercial transaction between providers and consumers including distance sales. Therefore, the LFPC could be applied to mobile commerce in general and specifically mobile commerce in Mexico could be regulated

provisions of the Distance Selling Directive 97/7/EC apply in most cases. Telecommunication acts also regulate quality of mobile services (*e.g.* Germany, Poland).

Unsolicited sales

Some countries actively apply existing provisions of consumer protection acts to claims involving mobile commerce. In the case of unsolicited sales of mobile content through a mobile phone in Germany, Section 241a of the German Civil Code (BGB) protects consumers against the consequences of delivery of unordered goods or services. In Belgium, the consumer protection act assimilates this kind of practice to "*achat forcé*".[64] The European Commission's Unfair Commercial Practices Directive (2005/29/EC) also covers unsolicited sale of mobile content.

Non-delivery or incomplete download

Consumers may fail to receive products ordered through a mobile phone or be charged for mobile content that could not be completely downloaded. The main measure in this case is a cooling-off scheme. In Korea, for instance, the Act on Consumer Protection in Electronic Commerce (CPEC) obliges businesses to deliver products within three working days after receiving payment from consumers or to provide a refund within three days. In the United States, the Federal Trade Commission's Mail or Telephone Order Merchandise Rule may apply to purchases made through mobile commerce. This rule states that businesses must have a reasonable basis for stating or implying that they can ship within a certain time.

Self- or co-regulation

In many member countries, including Australia, Austria, Canada, Denmark, Finland, Korea, Norway, Sweden, the United Kingdom and the United States, self- or co-regulatory codes or other schemes have been developed by industry. For example, in the United States, the Mobile Marketing Association (MMA) adopted six principles in its code of conduct for mobile marketing.[65] One is that the consumer must receive and/or be offered something of value to them in return for receiving the communication. In order to avoid unsolicited sales, consumers must be allowed to opt into all mobile messaging programmes.

In Canada[66] and Denmark,[67] industry has taken the lead in adopting self-regulatory initiatives for premium content services through mobile devices. Australia has also been developing a more comprehensive framework for self-regulation of mobile premium services. The Australian Communications Authority, now part of the Australian Communication and Media Authority (ACMA), issued a determination in June 2005, which introduces rules for these services and encourages industry to

---

through a chapter of the LFPC devoted to consumer transactions done through electronic and optical storage means (*e.g.* CD, DVD).

64 Article 76 of Act of 14 July 1991 on the practices of trade and information and consumer protection (LPC).

65 In addition, in May 2005, the MMA, in co-operation with the Cellular Telecommunications & Internet Association (CTIA) developed "Best Practices Guidelines for Cross-Carrier Mobile Content Services", which include a section on advertising and promotion (www.mmaglobal.com/bestpractices.pdf). The CTIA has its own guidelines "Consumer Code for Wireless Service" (files.ctia.org/pdf/The_Code.pdf).

66 Canadian mobile carriers with Canadian Wireless Telecommunications Association (CWTA) have an initiative to adopt common short code code of conduct (www.txt.ca/common.htm).

67 Denmark has a framework agreement on mobile content services by the Telecommunication Industries Association (www.teleindu.dk/t2w_358.asp).

develop a self-regulatory scheme.[68] The *Mobile Premium Services Self-Regulatory Scheme* has been developed and was approved by ACMA on 28 September 2006.[69] Carriage service providers and content service providers, who are not members of the ACMA approved self-regulatory scheme, are bound by the Default Scheme which was developed in the June 2005 determination. Both schemes entered into effect on 29 October 2006.

Cross-border cases

In the European Union and the EEA EFTA states, cross-border cases are treated according to the principles set out in the Injunctions Directive. In Nordic countries, the basic rules contained in a Position Statement (October 2002) of the Nordic Consumer Ombudsman on e-commerce and marketing on the Internet apply to mobile commerce. These countries also agreed on a joint Position Statement on mobile content services in March 2006.[70] On the other hand, in Japan, for unsolicited sales, deceptive information and SMS spam, the Specified Commercial Transactions Law applies only if both sellers and consumers are in a Japanese jurisdiction.

Information disclosure for small screens

What kinds of protection for adequate information disclosure do member countries have?

Legal protection

In general, consumer protection laws require businesses to provide adequate information about commercial transactions in a clear and comprehensible way. In Australia, failure to disclose or inadequate disclosure can be subject to the misleading and deceptive conduct provisions of the Trade Practices Act. In Mexico, the Federal Law of Consumer Protection (LFPC) obliges businesses to provide accurate, verifiable information that is neither misleading nor abusive (Chapter III, art. 32). They are also to provide the total amount to be charged (art. 7bis), postal address, telephone numbers, and other relevant information such as the terms and conditions, costs, additional charges and payment forms (art. 76bis). In addition, the LFPC (art. 57) obliges service providers to make tariffs available to the public.

The Finnish Consumer Protection Act obliges business to provide information to consumers in a way suitable for the means of distance communication used (Chapter 6, sec. 13, "Door-to-door selling and distance selling"). In the case of mobile commerce, some flexibility is necessary because the limited capacity of the small screen may make it impossible to provide all details in a text message. However, the Finnish Consumer Ombudsman considers that merely giving an Internet address in an advertisement does not satisfy legal requirements because not all consumers have free Internet access. Moreover, if a consumer has not had an opportunity to read the contract terms before concluding the contract, the terms are not binding.[71]

---

68 Part 5 of the Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No 1) (www.acma.gov.au/acmainterwr/_assets/main/lib100039/mobile%20premium%20services%20determination%2029june05.pdf).

69 Further information on the scheme is available at www.commsalliance.com.au/projects/mobile_premium_services.

70 For example, www.forbrukerombudet.no/asset/2305/1/2305_1.pdf (in Norwegian)

71 It is based on the guidelines of the Finnish consumer ombudsman. See: www.kuluttajavirasto.fi/user_nf/default.asp?site=36&tmf=9770&lmf=9781&id=17326&mode=readdoc.

In Norway, the Consumer Ombudsman's Guidelines on Mobile Content Services (the CO guidelines)[72] specify minimum information disclosure: price, name of supplier, notification to stop (on-off services), any age limitation, contact details and supplier's customer service phone number. For subscription services, information such as subscription period and/or frequency of subscription, right to use content services, and number of messages expected should also be provided.

In Korea, information disclosure for small screens has not caused serious problems, but the Korean Consumer Protection Board has proposed improvements (*e.g.* notification by e-mail and reconfirmation by consumers) to the government.

Self- or co-regulation

In the United States, the Mobile Marketing Association has "Consumer Best Practices Guidelines for Cross-Carrier Mobile Content Services". With regard to promotion programmes, the Guidelines state that content providers should ensure, for example, that service pricing information is clearly and conspicuously indicated and "Help" messages clearly display the opt-out information. In Canada, the E-Commerce Code sets the general rules for information disclosure[73] and the Short Code Code of Conduct requests members to provide information such as identity, opt-out information, price, "Help" and "Information" functions, as well as the date and time at which the information was produced.

Unauthorised use

What kinds of protection schemes for unauthorised use of mobile phones do member countries have?

Protection under the terms of contracts

When a mobile device is lost or stolen and then used by an unauthorised person, liability for unauthorised use is allocated on the basis of the contract between mobile carriers and consumers in a number of countries, including the Czech Republic, Mexico, Norway, the Slovak Republic, Poland and Switzerland. Poland and the Slovak Republic, for example, have no legal protection against unauthorised use or liability for unauthorised charges, but mobile phone companies can block SIM cards and the International Mobile Equipment Identity (IMEI)[74] when consumers inform them that the device has been lost or stolen. PIN codes and the blocking of outgoing and incoming calls may also prevent unauthorised use. In Norway, if a mobile phone has been reported stolen to the carrier, the consumer is not liable for all charges registered. The exact allocation of liability depends on the contract.

Telecommunication protection

In Finland, section 76 of the Communications Market Act provides that a telecommunications operator is obliged to close a connection or prevent the use of a telephone if the user or other appropriate entity reports that a mobile phone or smartcard used in managing a mobile telephone has been lost and requests that the connection be closed or the use of the telephone prevented. Some Finnish carriers also have self-regulatory initiatives to place limits on bills. In addition, the Ministry of Transport and Communication has now accepted a proposal for amendments to this act which will come into force in March 2007. One of the amendments will allow telecommunications firms and consumers to agree in the

72 See: www.forbrukerombudet.no/asset/1656/1/1656_1.pdf.

73 For example, principle 1.1 mentions that vendors shall provide consumers with sufficient information to make an informed choice about whether and how to complete a transaction.

74 The IMEI is a 15-digit unique identifier allocated to each mobile phone device. It consists of a 6-digit type approval code (TAC), a 2-digit final assembly code (FAC), a 6-digit serial number (SNR) and a spare digit.

contract on a specific usage limit to prevent an uncontrolled increase in the amount of the invoice (*e.g.* use abroad and new services for which the costs are difficult to estimate).[75] Also, a consumer will only be liable for use without consent if he or she has been negligent, as in a case of unauthorised credit card use. In Sweden, a proposal to oblige all operators to offer their customers the option to block certain numbers and calls and to fix a ceiling for their telephone bills is under consideration by the government.

Payment cardholder protection[76]

Canada, Sweden and the United States report that payment card protection may cover some cases of unauthorised use. Denmark is a special case because the SIM card in mobile phones is explicitly regarded as a means of payment like other payment cards covered by the Act on Certain Payment Instruments. According to the act, the issuer is liable to compensate the holder for any loss caused by unauthorised use of the mobile SIM card.[77]

Another interesting example comes from the United Kingdom. The "Immobilize" campaign stresses that stolen phones will not work and encourages consumers to report thefts. [78] The reported information can help consumers to complete an insurance claim for unauthorised use although the main objective is to reduce the level of street crime.

SMS spam[79]

Most antispam acts or provisions cover spam via SMS (*e.g.* Australia's Spam Act 2003, Belgium's Act of 11 March 2003 on electronic commerce, the Czech Republic's Act on Some Services of the Information Society, the Slovak Republic's Act on Advertising and on Electronic Communication, Norway's Market Control Act, sec. 2b, the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM Act), and the European Union's Directive 2002/58/EC). If the mobile phone user does not accept to receive information-based advertisements, such advertisements will be considered spam.[80]

---

75 The Finnish Communications Regulatory Authority has defined specific blocking categories for public mobile networks and SMS messages. Services indicated with service numbers are classified according to their contents as *i)* general services, *ii)* consulting and ordering, *iii)* entertainment, and *iv)* adult entertainment. A consumer can choose which calls/messages he or she wishes to have blocked.

76 See also OECD (2001) and OECD (2005a), especially pages 10-15.

77 The Act describes five exceptional cases, one of which is use of the secret code. In such cases, the consumer is liable up to a maximum of DKK 8 000 (around USD 1 280 and EUR 1 070).

78 The campaign was launched in January 2005 and is supported by the mobile phone industry through the Mobile Industry Crime Action Forum, the National Mobile Phone Crime Unit in the Metropolitan Police Service, and 38 other UK police forces. In 2005, Immobilize holds the details of around 10 million phones for which mobile holders registered their IMEI number. It gives some advice for mobile phone crime prevention at its homepage. See: https://www.immobilise.com/home.ikml.

79 The OECD's special Spam Task Force analyses SMS spam and issued the council recommendation on cross-border enforcement co-operation in conjunction with the ICCP and the CCP. See DSTI/CP/ICCP/SPAM(2005)3/FINAL.

80 Consumer groups such as TACD have focused on the requirement of explicit authorisation, noting that consumers otherwise risk being deluged with unsolicited offers via their mobile phones. Further, the TACD recommends preventing all unsolicited advertisements for products and services from being sent to consumers' mobile phones (TACD, 2005).

Self-regulation by telecommunication operators is also an effective way to combat spam to mobile handsets. Operators commonly use filtering functions to deny reception of SMS that include URLs and phone numbers in the text. Among other measures, mobile carriers in Japan limit the number of e-mails sent and suspend lines of spammers using SMS and Internet e-mail to mobile devices.[81] In Switzerland, mobile carriers have introduced "interworking fees", which they charge on SMS entering their network in order to limit the amount of incoming mobile spam.

International industry efforts are also important for combating SMS spam because mobile spam is sent across networks and/or internationally. The GSM Association (GSMA) has developed information and recommended procedures to help mobile operators work together to identify and address this problem, and has set up international working groups on mobile spam. This facilitates international co-operation and the exchange of best practices among operators. The GSMA has also developed a non-legally binding Mobile Spam Code of Practice which was signed by 15 mobile operators in February 2006. The International Chamber of Commerce (ICC) issued a Code of Advertising and Marketing Communication Practice in September 2006, which mentions that unsolicited marketing communication should be sent only when there are reasonable grounds to believe that consumers will have an interest in the subject matter or offer (art. D5).[82]

Protection of minors

The high penetration rate of mobile phones among minors raises particular mobile commerce issues. Some commentators have noted that problems relating to minors' use of mobile devices sometimes cause a breakdown in family relationships and, as a consequence, require a strong advocacy response.[83] The main risks for minors in terms of mobile commerce are described below.

What is the legal situation of minors who engage in transactions?

In many countries, parental consent is required to allow minors to engage in commercial transactions. In Japan, the Civil Code provides that a minor shall obtain the consent of a legal representative when undertaking a legal act and that any act performed without such consent may be revoked. In Finland, according to the Guardianship Service Act, sec. 23 and 24, persons under the age of 18 have limited legal competence and can only perform ordinary transactions of little significance. Minors do not have the right to incur debt; they can only perform cash transactions. Purchases made by mobile phone are billed afterwards. When service providers target children with special marketing and develop new services aimed at children, parents should not have to bear full responsibility for every possible situation. A service provider must take into account that a minor is not the same kind of contract partner as an adult. There is also the question of telecommunication operators' right to charge for transactions that are not considered valid.

Some countries have provisions prohibiting minors under a certain age from concluding a contract even if they have obtained parental consent. In Belgium, for instance, those under 18 years of age cannot engage in contracts (Civil Code, sec. 1124). In Germany, according to the Civil Code (BGB), children under age 7 are incapable of making a contract (BGB, sec. 104), while persons between 7 and 18 years

81 The Finnish Communications Regulatory Authority also states that, in order to ensure the information security of services, an operator may prevent transmission of information and receipt of messages, remove malicious software that endangers information security from messages and undertake comparable technical measures.

82 See: www.iccwbo.org/policy/marketing/id8532/index.html.

83 Mr. Denis Nelthorpe, Consumer Law Centre Victoria, Australia, mentioned this at the experts' meeting on children, mobile phones and the Internet, 6-7 March 2003. See IAJ (2003).

may only conclude a contract with parental consent (BGB, sec. 1106). In Hungary, all contractual actions for children under the age of 14 have to be taken by a parent; children between 14 and 18 years of age require parental consent before or after their action. In Poland, a contract made by minors under age 13 is void; and a contract by a person between 13 and 18 years of age is valid only with parental consent.

How do the member countries deal with over-consumption by minors?

Many countries provide that a parent or a legal guardian has the right and duty to answer for legal acts of children living with them (*e.g.* in Mexico, Civil Code art. 1919; in Germany, BGB. art. 1626 subsection 1).

Although no member country has legal provisions dealing specifically with the level of consumption of minors, regulators in some countries aim to ensure that businesses' marketing and contract terms comply with relevant regulations. For example, in Norway, parents have legal responsibility for minors, but the CO guidelines contain some lists that businesses should follow on the marketing and sale of mobile content services to minors.[84] In Chapters 5.4 and 5.5 of the guidelines, the Ombudsman states some ceilings for services targeting minors. For example, the Consumer Ombudsman may consider a violation of the Marketing Control Act (MCA) to have occurred if content suppliers do not set a monthly limit of about NOK 1 000 (USD 145 and EUR 125), including VAT, for the purchase of services from an access number. Also, for subscription services, there is a ceiling of NOK 100. The Finnish Consumer Ombudsman also emphasises service providers' responsibility to provide fair and legal services when their marketing targets minors, even though parents have legal responsibility as guardians. In Korea, the Act on Consumer Protection in Electronic Commerce requests businesses to inform a minor that the contract can be cancelled by the minor or the parents if the parents do not consent to undertake the contract.[85]

Industry also has developed codes of conduct. In Canada, the Canadian Code of Practice for Consumer Protection in Electronic Commerce and the Short Code Code of Conduct are relevant. The former prescribes that vendors shall take all reasonable steps to prevent monetary transactions with children. The latter prescribes that the programme aggregator must verify that each end user is of legal age in his/her residence, before allowing him/her to participate in the programme or to receive a message. In the United Kingdom, telecoms operators, including mobile operators, agreed a voluntary Memorandum of Understanding (MoU) for the purpose of monitoring traffic and sharing information after a review of prime rate services by the Office of Communications (Ofcom).

Technological measures are also common. In Australia, a PIN number is commonly used to restrict access by children to adult content services such as telephone sex services. Another measure includes age verification to ensure children do not have access to adult services. Mobile phone operators are examining ways of registering phones owned by minors under 18 years of age so that the phones are unable to access adult material. In Japan, the E-Commerce Guidelines (METI, 2006) indicate that it may not be sufficient for business simply to provide age verification in order to apply the concept of *fraudulent information* by minors in section 20 of the Civil Code.

What kinds of protection scheme do member countries have regarding access to inappropriate services by minors?

Only one country reports a comprehensive regulation on all services to minors. Quebec's Consumer Protection Act in Canada prohibits businesses from marketing to children under age 13.[86] Elsewhere, there

84 www.forbrukerombudet.no/asset/1656/1/1656_1.pdf.

85 Sec. 13, subsection 3, added when the act was amended in 2005.

86 See sec. 248 at: www.canlii.org/qc/laws/sta/p-40.1/20060115/whole.html.

are regulations that protect minors from accessing some kinds of content (Australia, Finland, Germany, Korea, Mexico, the Slovak Republic and Switzerland). Switzerland's Penal Code prohibits distribution of pornographic material to minors (16 years of age or less).[87] Australia's Criminal Code Act 1995 prohibits the sending or obtaining of child pornography and the sending of pornography to a person under 16 years of age for the purpose of attracting a child.[88] In Mexico, art. 76 bis of the LFPC is also applicable to the issue. The provision establishes that providers must avoid using selling or advertising strategies not giving consumers clear and enough information about the offered services, particularly in cases of marketing practices directed to vulnerable person such as children, the elderly and the sick, including mechanisms to advice them when information is not appropriate for these group.

Regulatory guidelines can also be used to regulate content services. For example, based on marketing and contract terms in the Consumer Protection Act, Finland's Consumer Ombudsman issued guidelines for services targeting minors.[89] They specify that on Internet pages targeted at minors, functions or material that are unsuitable for children or young people should be removed. With regard to websites attracted to children and young people, the guidelines state that content should be clearly separate from material that is only suitable for adults. In a court case in early 2004, the Ombudsman reached an agreement with a provider of mobile text messages targeting minors to impose a weekly limit and to inform parents by e-mail that their child had signed up for the services. In Norway, the CO guidelines also address this issue.[90]

Self-regulation of mobile content is also widely used in OECD countries. For example, articles 18 and D7 of the ICC's code of conduct relate to the protection of minors. While they are not limited to mobile commerce, they state that special care should be taken when marketing to or featuring children or young people.[91] In the United Kingdom, mobile operators deal with this matter through their code of practice on content.[92] For commercial content (*e.g.* films, games), except premium rate voice or texting services, they follow the framework developed by the Independent Mobile Classification Body (IMCB). For premium

---

87 See art. 197 at: www.admin.ch/ch/f/rs/311_0/a197.html. In Germany, sec. 184 and 184c of the Criminal Code (*Straggesetzbuch- StGB*) aim to protect minors from being confronted with pornographic content.

88 The Department of Communications, Information Technology and the Arts examined mobile internet access by minors and filtering requirements in pages 106-112 of DCITA(2006). In addition, the Minister, Senator Helen Coonan, announced on 22 August 2006 that she would soon introduce to Parliament legislation to extend the current safeguards for minors over the Internet or television to content delivered over convergent devices such as mobile phones. The new law will include prohibition of adult content rated as well as requirements for consumer advice and age-restrictions on access to content suited only to adults. These prohibitions will be backed by sanctions for non-compliance with the new regulatory framework, including criminal penalties for serious offences. See: www.minister.dcita.gov.au/media/media_releases/content_safeguards_extended_to_mobile_phones.

89 The Consumer Ombudsman's guidelines (minors, marketing and purchases). See: www.kuluttajavirasto.fi/user/loadFile.asp?id=5603.

90 Section 4.1 provides that mobile content services must not be marketed to children and young people if the content is unsuitable for this age group (*e.g.* frightening, violent, erotic/pornographic). Section 4.2 discusses information disclosure concerning age limits. See: www.forbrukerombudet.no/asset/1656/1/1656_1.pdf.

91 More specifically, it declares that products unsuitable for children or young people should not be advertised in media targeted to them, and advertisements directed to children or young people should not be inserted in media where the editorial matter is unsuitable for them. See www.iccwbo.org/policy/marketing/id8532/index.html.

92 UK Code of Practice for the Self-regulation of New Forms of Content on Mobiles (19 January 2004) by O2 (UK), Orange Personal Communications Services, T-Mobile UK, Virgin Mobile Telecoms, Vodafone, and Hutchison 3G UK.

voice or texting services, they operate under the ICSTIS Code of Practice. Ofcom provides statutory support to the work of ICSTIS. Each mobile operator has to place content classified as "18" (*i.e.* inappropriate for minors) behind access controls and only make it available to customers when it has satisfactorily verified that the customer is 18 years old or more. On the other hand, because mobile operators have no control over the content offered on the Internet, the code recommends that they apply a filter to their Internet access service. Lastly, for illegal content, the code recommends that it be reported to law enforcement agencies. Furthermore, if such content is placed where the mobile operator can control it, the code recommends that it should take action based on its "notify and take-down" provision.

The United Kingdom's code of practice also addresses filtering of content. It covers new types of content, including visual content, online gambling, mobile gaming, chat rooms and Internet access. For example, carriers classify each carrier's commercial content and provide filtering systems to parents who can set filtering function for Internet sites for their children. Also, they have designated an independent body to set classification standards, provide advice to content providers and handle complaints of misclassification. In Denmark, a framework agreement for mobile content services was set up by the country's telecommunication operators.[93] Service providers must comply with the agreement and use the associated application codes when they offer mobile content services. Japan's Ministry of Internal Affairs and Communications (MIC) has been examining filtering technology applicable specifically to mobile commerce since 2004.

In Germany, to protect minors against illicit, pornographic or other content that is seriously harmful to young persons and to allow parents to block access to their children's mobile phones, all major mobile carriers have issued a joint code of conduct. For instance, they commit to providing an age verification system.[94] In addition, the Youth Media Protection Interstate Treaty (*Jugendmedienschutz- Staatsvertrag, JMStV*), which entered into effect in April 2003, applies to mobile content. The main supervisory organisations are the Commission for the Protection of Minors from Unsuitable Media Content (*Kommission für Jugendmedienschutz* – KJM), and the voluntary self-regulatory organisations (SKEs) certified by KJM. In the United States, the Dot Kids Implementation and Efficiency Act of 2002 was implemented to provide "www.kids.us", a website to encourage online safety for children under 13. NeuStar is responsible for developing guidelines and restrictions to ensure that content on Kids.us sites are both "suitable for minors" and not "harmful to minors".

What kinds of information and education campaigns have taken place in member countries?

Information materials and education campaigns have been widely used in member countries to protect minors. In Germany, the Thuringia Consumer Advice Centre (*Verbraucher-Zenrale Thüringen e.V*) made a CD-ROM, "Achtung Taschengeldgangster", for children aged 10 to 12 and provides them free of charge at all consumer advisory boards. The Centre also produced a booklet "Computer, mobile phone, TV and Co." to handle issues relating to television and video on computers and mobile phones. Also, in Germany, a "handybooklet" is being planned by the Berlin debtor advice centre with the Federal Minister of Food, Agriculture and Consumer Protection (BMELV). In Poland, an information leaflet on mobile commerce

93 www.teleindu.dk/t2w_358.asp.

94 www.t-mobile.de/downloads/t-mobile_broschueren/t-mobile__verhaltenskodex_der_mobilfunkanbieter_in_deutschland_zum_jugendschutz_im_mobilfunk.pdf. Another code of conduct was issued in Germany in 2003 by an association of premium rate services industries (*Verhaltenskodex des Vereins Freiwillige Selbstkontrolle Telefonmehrwertdienste e.V.*), which includes general rules of conduct and recommendations on how to provide premium rate services for members. However, the code does not establish any standards beyond the statutory provisions.

and junior consumers ("*Telefonia komórkowa a mlody konsument*") was produced by OCCP in 2004.[95] In Switzerland, the communications regulator, the Federal Office of Communications (OFCOM), produced a booklet, "SMS messages that cost", in June 2005. These materials mainly give information about potential threats, how to manage costs, how to prevent abuse and whom to contact in case of problems. In Finland, the Consumer Agency often provides information concerning mobile commerce in their magazine, the KULUTTAJA, and on their website. As a joint project, Nordic ombudsmen are planning to launch an online game called "Nordic Galactor" in early 2007 to teach children and young adults about important principles and risks concerning electronic and mobile commerce and other information society services. In Australia, the Australian Competition and Consumer Commission (ACCC) provides mobile commerce tips for consumers on their website.[96]

Private companies and industry organisations are also involved in the development of leaflets. For example, the National Family and Parenting Institute in the United Kingdom produced with Vodafone a guide for parents.[97] In Austria, in addition to the government's guide for youth issued in September 2003,[98] the Austrian Red Cross Youth and a lawyers' group (*Kinder- und Jugendanwaltschaft Wien*) produced with Mobilkom Austria a leaflet for children.[99] In Australia, NetAlert, an Internet educational body funded by the government, is providing safety information on "mobile Internet enhanced devices" for parents.[100] The Australian Interactive Media Industry Association (AIMIA) is also going to start a "Mobile Content Consumer Education Campaign" through television and press advertising, in-store brochures, website and a mobile site in order to ensure that consumers have positive experiences with mobile content.[101] In Japan, the industry, in co-operation with ministries, has set up the so-called "E-net Caravan", which provides lectures for parents and teachers to teach how to use the Internet and mobile phones safely and with confidence.[102]

---

95 The 2006 version (Polish only) is available at: www.uokik.gov.pl/download/Z2Z4L3Vva2lrL3BsL2tzZ19weXRhbmlhLnYwLzEzMC8yMS8xL3RlbGVmb25pYV9rb21vcmtvd2EucGRm.

96 www.accc.gov.au/content/index.phtml/itemId/266899/fromItemId/8135.

97 www.family-parenting.org/Bullying/StayingInTouch-ParentsGuide.pdf.

98 "Der Handy-Guide –Alles was Recht ist" by the Federal Ministry of Social Security, Generations and Consumer Protection (BMSGK). See: www.bmsg.gv.at/cms/site/attachments/2/9/3/CH0036/CMS1091089868037/handybroschuerear5.pdf (German only).

99 "Handy Guide – Alles rund ums Telefonieren mit dem Handy" (German only). See: www.mobilkomaustria.com/CDA/getAttachment_mk/0,3148,1048,00.handy_guide.pdf.

100 www.netalert.net.au/02349-Mobile-Internet-Enabled-Devices.pdf.

101 Press release of 31 August 2006. See: www.aimia.com.au/i-cms?page=2299.

102 www.fmmc.or.jp/e-netcaravan/ (Japanese only).

IV. PRIVACY AND SECURITY ISSUES

The development of mobile services provides obvious benefits to consumers and is a huge growth area for service providers.[103] However, a number of privacy and security issues need to be addressed as the technology develops. The OECD has been developing policy frameworks to foster a culture of security and privacy and to build trust in information and communication technologies (ICTs) for several years. These frameworks provide a backdrop for analysing the relevant issues.

More than 25 years ago, the OECD recognised that the rapid development of communications infrastructure and technologies raised new privacy issues. To address these issues, the OECD adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("Privacy Guidelines"). They provide guidance at national and international level with regard to the collection and processing of personal information and are relevant to personal information processed through mobile commerce.

The OECD's 2002 *Guidelines for the Security of Information Systems and Networks* ("Security Guidelines") guide the development of policies to help address security threats and vulnerabilities in a globally interconnected society, while preserving important societal values such as privacy and individual freedom. More broadly, they reflect a shared ambition to develop a "culture of security" across society, so that security becomes an integral part of the way that individuals, businesses and governments use ICT and conduct online activities, including mobile commerce.

This section examines a number of the privacy and security issues that have arisen in relation to mobile commerce. First, it looks at the impact of location-based services on mobile phone users' privacy. Second, it examines some of the security implications of mobile phones with Bluetooth technology and the threat viruses and worms pose to mobile phones. It also describes some of the measures already taken to address these issues.

Privacy issues arising from location-based services

Different technologies have been developed to determine a mobile phone's location. They can broadly be divided into three categories: one in which the mobile phone calculates its own location (GPS), another in which the mobile phone network calculates the location (Cell ID and triangulation of the location of the subscriber), and a third that combines two or more techniques (assisted GPS) (Steinfield, 2004). Partly driven by legal obligations, network operators in some countries have recently started to modify their networks to make more precise location information available for use by emergency services.[104] For instance, in the United States wireless carriers are required to identify the caller's location within 50 to 300 metres.[105]

---

103 See paragraph 21 page 11

104 In the United States under the *Wireless Communications and Public Safety Act* (the "911 Act") (1999); in Korea under Article 3s. (7) of the *Act on Disaster Preparedness & Safety Management* and Article 29 of the *Act on Protection and Use of Location-Based Services; and* in the European Union under Article 26 of the *Universal Service Directive* [Directive 2002/22/EC].

105 Under Phase 2 of the FCC's "Enhanced 911" Rules. See: www.fcc.gov/911/enhanced

Development of sensor networking and location-tracking technology make location information services possible. As most mobile phone users are *individuals*, the ability to locate a mobile phone precisely also makes it possible to locate an individual subscriber. As a result, location information is typically considered personal information and falls within the scope of protection afforded by privacy laws.

Earlier, location information was only generated and used to establish and maintain a connection to the mobile phone. It therefore resided solely with the operators of telecommunications networks, which are often bound by telecommunications privacy legislation.[106] However, the development of mobile commerce has led to the creation of a variety of new services based on knowledge about the user's precise location. As mentioned, location-based information services using GPS technology and other sensor networks have been identified as an important mobile commerce opportunity.

In addition, there are now location-based services that the user does not have to request. Such push "location-based advertising" allows messages to be sent to the user's mobile phone to provide, for example, special offers in restaurants and shops near the user's location.[107] While some users may find this information helpful, others may perceive it as an invasion of privacy.[108]

Therefore, it would be beneficial for the development of location-based services to identify the key elements for protecting the privacy of a user's location information. Commonly accepted rules or principles for how location information is collected, what use can be made of it and for how long it can be stored would provide important safeguards for the protection of the privacy of mobile phone users.

Obtaining consent

Consent is a key privacy issue raised by the development of location based services. What type of consent does the service provider need before processing a mobile phone user's location information? This question is particularly important for businesses engaging in location-based advertising.

The OECD Privacy Guidelines recommend (paragraph 7) that the collection of personal data, including location information for mobile users, should be obtained where appropriate with the knowledge or consent of the data subject.

A TACD resolution on mobile commerce recommends that the use of any personal data (including location information) for purposes that the consumer has not explicitly agreed to should be prohibited (TACD, 2005). The International Working Group on Data Protection in Telecommunications similarly advises that the user must remain in control of the generation of precise location information.[109] It recommends that location information should only be made available to providers of value added services if the user has given informed consent for such disclosure.

---

106 As in Australia, in Part 13 of the *Telecommunications Act 1997*.

107 See footnote 61 page 21

108 A related issue, whether location-based advertising constitutes spam, is discussed earlier in Part II of this report.

109 Since 1983, the Group has adopted various recommendations ("Common Positions" and "Working Papers") aimed at improving the protection of privacy in telecommunications. Membership of the Group includes representatives from data protection authorities and other bodies of national public administrations, international organisations and scientists from all over the world. See IWGDPT (2004).

In the European Union, Article 9 of the Directive on Privacy and Electronic Communications requires informed opt-in consent of the user for the provision of location-based services. [110] To obtain the user's consent, the service provider must inform subscribers about what kind of location information will be used, for what purpose and for what duration, and whether the data will be transmitted to a third party for the purpose of providing a service.

The EC Article 29 Data Protection Working Party (2005) subsequently clarified the conditions necessary for obtaining consent for processing location information under the Directive. According to the Working Party, consent cannot be given as part of the general terms and conditions for the electronic communications being offered.

The Working Party also noted that, depending on the type of service, consent may constitute agreement to be located on an ongoing basis provided users are given full information in advance about the processing of their location data. Further, the Working Party takes the view that providers of value added services must take appropriate measures to ensure that the consent remains valid. When the processing of location information is ongoing, the service provider should achieve this by confirming the user's subscription to the service by sending a message to the user's phone after consent has been received, and if necessary requesting confirmation of the subscription.

Given the sensitive nature of location information, the Working Party stresses the right of individuals who have given consent for the processing of location information to withdraw that consent at any time under the Directive on Privacy and Electronic Communications (2002/58/EC, art. 9). In the context of location-based advertising, it is noteworthy that the Directive specifically provides protection against intrusion of privacy caused by unsolicited messages sent to mobile phones for direct marketing purposes. Under Article 13.3 of the Directive, unsolicited communications for direct marketing purposes are not allowed without the consent of the subscriber.

Under federal legislation in the United States, location information is considered to be customer proprietary network information (CPNI), and can only be released with prior customer authorisation except in emergency situations.[111] Civil Society organisations such as the Center for Democracy and Technology have called on the Federal Communications Commission to clarify requirements for express prior authorisation before a service can be provided.[112]

Japan and Korea have set out guidelines for the protection of users' location information. In Japan, Article 11 of the 1998 *Guidelines on the Protection of Personal Data in Telecommunications Business* provides that a telecommunications carrier shall not disclose the location information to another except under certain condition such as "when the data subject gives consent".[113] These non-binding guidelines are perceived as having facilitated the rapid growth of the industry in Japan (Ackerman *et al*., 2003). Japan's Personal Information Protection Law places restrictions on the use of users' personal information

110 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 (Directive on privacy and electronic communications), at www.europa.eu/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

111 Section 222 of the *Communications Act* (1934), amended by *Wireless Communications and Public Safety Act* (1999).

112 www.cdt.org/privacy/issues/location/020406fcc.shtml.

113 www.soumu.go.jp/joho_tsusin/d_syohi/d_guide_01.html (Japanese only).

(including location information) and retains the requirement for informed opt-in consent in the 2004 guidelines.[114]

As of March 2005 Korea had 3.76 million subscribers using location-based services (OECD, 2005g). Korea has sought to protect location information by requiring service providers to send a text message to seek the user's consent before providing the service (Act on the Promotion of Information Network Utilization and Information Protection, art. 50, sec. 2). Articles 15 and 40 of Korea's new Act on the Protection and Use of Location-based Services reinforces the requirement for consent before location information is collected, used or provided and has provisions for criminal sanctions including jail time for violators.

Another factor affecting the validity of the consent is the already mentioned problem of the small size of mobile phone screens.[115] The issue here is what information service providers need to include in the message, given the limited capacity of the small screen.

Retention of location information and transmission to third parties

Various issues have arisen relating to what location information can be stored, how long the service provider is entitled to retain such information, and when such information can be transmitted to third parties. What information is stored is important because the amount of detail affects potential future uses of the information. How long information is stored determines many future uses of the information, particularly for long-term tracking and pattern recognition. For instance, if location information is recorded along with a sequence of authenticated transactions, the information can be linked to a particular user rather than simply to the mobile phone. The requirement of consent is particularly important when a service provider is entitled to transmit a user's location information to a third party in light of the service provider's duty to respect the private nature of the information.

The issue arises as to whether service providers or third parties may be able to build up a profile of the user, matching location information against other databases, which would constitute an invasion of privacy. For example, a car insurance company could charge a person a higher insurance premium because of the fact that he or she travels through a dangerous area regularly. The TACD argues that user profiling may also lead to more intrusive marketing (TACD, 2005).

Within the EU, the Directive on Privacy and Electronic Communications specifically addresses these issues (EC Article 29 Working Party, 2005). Location information may only be processed for "the duration necessary for the provision of a value added service" [Directive 2002/58/EC, art. 9(1)]. As the EC Article 29 Data Protection Working Party (2005) notes, this means that the service provider may not in principle store the user's location information once the service has been provided. If service providers need to store a record of a user's location information, they must first render the data anonymous.[116]

However, Finland has noted that anonymous location information, which cannot as such or in association with other data be linked to a specific user, may be freely processed. A problem of

114 www.soumu.go.jp/joho_tsusin/d_syohi/pdf/051018_1.pdf (Japanese only).

115 See section "Information disclosure for small screens" in Part III, page 24.

116 In order to keep anonymity or to allow users to control information based on their preference of privacy policies, experts are proposing new system architectures to enhance privacy protection of location information. For example, Nakanishi et al. (2004) proposed that identity detectors should be separated from location-aware applications. Ahmad et al. (2004) proposed introducing an access control list and access management servers for geographic location information. Gakparia et al (2004) proposed that a trusted third party should involve in privacy control of location information.

interpretation can arise in relation to the question of when information is clearly anonymous and when in fact it may be clearly linked to certain subscribers or users. A situation of this kind can arise, for example, when the number of persons located is small or the limited area in which they move is known in advance. Only telecoms companies and mobile service providers whose task it is to handle this information may process location information. Nevertheless, Finland argues that there is a risk of location data being processed by persons who are not entitled to do so or of data obtained with the aid of positioning technology being used for purposes that constitute an invasion of privacy (OECD, 2004c).

Under Article 9(1) of Directive 2002/58/EC, the service provider must also inform users prior to obtaining their consent of the type of location information to be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing a value added service. It further provides that location information may not be transmitted to third parties other than those providing the value added service (art. 9(3)).

Unlike the EU, which has adopted a regulatory approach, the United States' FCC has chosen not to issue rules on location information practices on the grounds that location-based services are still in their infancy and the FCC does not wish to constrain technology or consumer choice by adopting rules (FCC, 2002). However, there have been self-regulatory efforts in the United States. For example, the Mobile Marketing Association and the Cellular Telecommunications and Internet Association have provided guidelines which address location information protection.[117]

On the business side, many service providers include these issues in their privacy policies. For example, a UK mobile operator, O2 UK provides a Location Services Privacy Controller (LSPC) so that consumers may refuse to have their location information disclosed for some or all services.

While approaches differ from country to country, there appears to be a general sense that clear, unambiguous consent for the collection and use of a person's location information is an important element of privacy protection. This is consistent with the approach taken in the OECD Privacy Guidelines.

Security issues

Although privacy issues have tended to attract greater attention, security issues also need to be addressed for mobile commerce to reach its potential. This is particularly the case for mobile phones with built-in infrared (*e.g.* IrDA), or radio frequency technology [*e.g.* Blueooth, RFID tag and contactless (or proximity) card], which are already used as a payment method in some countries.[118] The following section focuses on Bluetooth technology.[119] Further, the possibility that viruses or worms may affect mobile phones on a widespread scale in the future has become a matter of some concern.

Security issues raised by Bluetooth technology

Bluetooth technology is increasingly included in mobile phones. It utilises radio frequency waves to communicate wirelessly between Bluetooth-enabled devices. For example, users may send business cards

117 The MMA and the CTIA have developed "Best Practices Guidelines for Cross-Carrier Mobile Content Services" (www.mmaglobal.com/bestpractices.pdf). The CTIA has its own guidelines "Consumer Code for Wireless Service" (files.ctia.org/pdf/The_Code.pdf).

118 See Part II on technological development in this report. Contactless (or proximity) cards are used for integrated mobile financial services. Therefore, the security of contactless cards is a key issue when payment security issues are discussed though it is not mentioned in this report.

119 Hacking into other technologies can also happen (side channel attack and crypt-analysis). See, for instance, Witteman (2006); Handschuh (2004); http://cq.cx/proxmark3.pl.

to other users' mobile phones or use a wireless headset to talk on their mobile phone. In the United States, 11% of consumers have this feature and 45% of them have used it (Rockbridge Associates and Robert H. Smith School of Business, University of Maryland, 2006). Moreover, 30% of consumers wish to have the feature.

A security feature of Bluetooth-enabled mobile phones is that they will not communicate until they have "paired". This is a one-off process in which both devices must enter the same PIN number. Along with the Bluetooth's short range (generally 10 metres in mobile phones; Whitehouse, 2003), this process helps limit the possibility of a security breach.

Hackers have attempted to gain improper access to information on users' mobile phones using Bluetooth technology. The ability of hackers to access information contained on a person's mobile phone raises both security and privacy issues. "Bluejacking" was one of the first improper uses of Bluetooth technology. It allows mobile phone users to use Bluetooth technology to send business cards anonymously to other mobile phones. Bluejacking does not pose a security threat to the receiver of the business card, in that data in the mobile phone are not removed or altered. Nevertheless, Bluejacking can be seen as invasive, especially if the message contains abusive or threatening language.[120]

"Bluesnarfing" is the term used for techniques developed to steal information such as phonebook contacts and calendar information from a phone (Laurie *et al*., 2004). The hacker must be running a device with specialised software and generally be within 10 metres of the mobile phone. Only certain older generation Bluetoooth-enabled mobile phones are vulnerable to Bluesnarfing. However if these mobile phones are set to "non-discoverable" it will be much more difficult for hackers to access the user's information. Therefore, most of the security issues raised by Bluesnarfing have been addressed.[121]

Other Bluetooth vulnerabilities include – at least theoretically – the possibility that hackers could crack the security codes on Bluetooth-enabled devices and seize control of them (Shaked and Wool, 2005), although this seems to be limited to mobile phones using a "custom Bluetooth device" [122] and could not be accomplished using off-the-shelf components. However, users should be aware of these risks and protect themselves by using an eight-digit instead of a four-digit PIN to minimise the risk of hackers cracking the security code.

As highlighted in Principle 1 of the OECD *Guidelines for the Security of Information Systems and Networks,* the first line of defence against security problems is awareness of the risks and available safeguards. Because workers now store confidential business information such as contact lists, e-mail and passwords on their mobile phones, employers should ensure that they are aware of what they can do to enhance security. In the United States, for example, the National Institute of Standards and Technology has issued a Bluetooth security checklist with guidelines for maintaining a secure Bluetooth network (Karygiannis and Owens, 2002). In addition, the United States Computer Emergency Readiness Team[123] and the Bluetooth Special Interest Group (Bluetooth SIG, 2006a) have issued guidelines for users about how to secure mobile phones against the possibility of such attacks.

---

120 Bluejack Q, "What is Bluejacking?" See: www.bluejackq.com

121 Another technique, "Bluebugging", makes it possible to access mobile phones with Bluetooth technology without the owner's knowledge and initiate phone calls or listen in on phone conversations, among other things. However only a few Bluetooth models were vulnerable to Bluebugging and the manufacturers of have since corrected the problem. See the Bluetooth Special Interest Group website, www.bluetooth.com/Bluetooth/Learn/Security/.

122 www.bluejackq.com

123 McDowell, M., Lytle, M. (2005) "Understanding Bluetooth Technology"

Common recommendations include disabling Bluetooth when not using it and making sure that when Bluetooth is enabled it is in non-discoverable mode. Users should also be aware of their environment when using Bluetooth technology. There is a greater risk of someone intercepting a Bluetooth connection in a public wireless hotspot than in a private setting. Users are therefore advised against pairing Bluetooth devices in public places. Furthermore, they should use at least an eight-digit PIN and should only share it with trusted individuals. Provided users are aware of the risks and take these precautions, Bluetooth technology is considered comparatively secure.

Manufacturers of mobile phones with Bluetooth technology can also take steps to address security risks and should respond in a timely manner to address security incidents (Principle 3 of the OECD Security Guidelines). Manufacturers did in fact identify vulnerabilities in the Bluetooth technology on certain mobile phones and developed software upgrades to fix the problem (Bluetooth SIG, 2006b). Mobile phone manufacturers should continue to conduct risk assessments to identify threats and vulnerabilities in Bluetooth technology and take preventive measures (Principle 6 of the OECD Security Guidelines).

The risk of viruses and worms

There has been increased concern regarding the security threat posed by viruses to mobile phones (IBM, 2005). Although some have questioned how serious the threat may be (IBM, 2006), the fact that mobile phones now contain important financial data and exchange information that criminals may seek to obtain means that the issue of mobile viruses is generating debate.

Until recently reports of infected mobile phones were very rare. This is partly because Internet-connectable phones accounted for only a small percentage of the mobile phones in use, especially before 3G mobile phones come into the marketplace. Other factors include the diversity of operating systems used by manufacturers, which makes it more difficult for viruses to spread (Cousins, 2005). Some analysts consider that viruses and worms will not be able to infect large numbers of mobile phones until at least 30% of all mobile phones are Internet-connectable phones and users regularly exchange executable files. This is not forecast to occur until the end of 2007 at the earliest (Pescatore and Girard, 2005).

Despite the currently low level of risk, the number of viruses targeting mobile phones is increasing. For example, Trend Micro reports having received 104 virus reports associated with mobile phones up to March 2006 (*e.g.* Cabir, QDial, RedBrowser and Mabir).[124] F-Secure, a provider of antivirus products, recently announced that there are now more than 200 mobile viruses in circulation (F-Secure, 2006). Mobile viruses can spread in a number of ways, such as via malicious websites, e-mail attachments, Bluetooth and SMS text messages.

For example, RedBrowser is a Trojan horse. Instead of retrieving WAP pages to send free SMS e-mail, it sends SMS messages for premium rate services for which users are charged high rates. Mabir, Commwarrior and other viruses use MMS and can spread through mobile networks. Compared to viruses that only spread via Bluetooth, the scope for infecting devices increases. Most viruses currently only affect mobile phones using the most widely used Symbian OS-based operating system.

Also, the user has to accept messages containing viruses before they infect the phone. However, according to analysts, owing to users' lack of knowledge about the threat of mobile phone viruses, they are more likely to open such messages than when they receive an e-mail on a PC which raises a number of "red flags" they are unlikely to miss. Analysts also believe that those who write viruses for mobile phones will increasingly look for ways to profit from their hacking (Cousins, 2005).

---

124 See Trend Micro (2005) about history and characteristics of mobile virus.

What can manufacturers and users do to prevent the spread of mobile viruses? Some mobile phone operators have begun to focus on the network, scanning messages in order to filter malicious programmes (Evers, n.d.). Mobile devices now have pre-installed antivirus software (*e.g.* Nokia 6670, Nokia 9500, and NTT DoCoMo 901i). Software companies also provide security software for mobile devices (*e.g.* McAfee Security Scan, Trend Micro Mobile Security, Symantec Client Security and F-Secure Mobile Anti-Virus).

However, all participants must take responsibility for the security of mobile phone operating systems and must be in a position to react in a timely manner to prevent, detect and respond to security incidents (Principles 2 and 3 of the OECD Security Guidelines). In particular, manufacturers and users must be aware of the risks posed by viruses to mobile phones (Principle 1 of the OECD Security Guidelines). Whether or not users install software to protect their mobile phones they should always exercise caution when accepting applications or opening MMS attachments, particularly from an unknown source. They are also well-advised to disable Bluetooth when not using it. They must be made aware of these risks and manufacturers have begun to take steps to warn users of the risk posed by viruses (Nokia, 2005).

In addition, according to Pescatore and Girard (2005), antivirus tools, although useful for removing viruses, do not provide adequate protection, and more emphasis needs to be placed on building protection into the network. According to Hicks (2006), the ICT industry now acknowledges the need for more secure computing models for mobile operating systems.

As the market for mobile phones is projected to grow rapidly, participants should continue to assess the risks to the security of the system (Principle 6 of the OECD Security Guidelines). Risk assessments help to anticipate the potential harm that may be caused by viruses to the operation and development of mobile phone technology and can be of assistance in selecting appropriate controls.

CONCLUSION

To protect consumers, regulation of mobile commerce requires a mix of government initiatives and business self-regulation, as well as approaches that make use of technology development and information and awareness raising. Parents also have an important role to protect minors. OECD member countries evaluate the success of existing efforts differently. Some believe that current regulations are sufficient to resolve most mobile commerce issues. Others feel that current regulations are not sufficient to resolve all relevant issues because they cannot always be easily applied to the rapidly evolving technologies.

The results of surveys conducted in member countries reveal some gaps between expectation and reality in spite of legal protection and intensive business efforts. For example, 53.4% of teens reported having accessed pornography services by registering under their parents' ID number;[125] 60.0% of students 13 and 14 years old have not told their parents that they have used mobile dating services (National Congress of Parents and Teachers Association of Japan, 2005); 31% of the mobile sites examined do not give sufficiently clear information about prices, and 22% do not give information about how a child can stop a subscription.[126] Among consumers who lodged complaints about problems related to mobile commerce, 50% said they were unable to successfully resolve them (TACD, 2006). These results reveal the extent of policy challenges to be faced.

Consumers in developing countries are rushing into the mobile market because mobile phone subscriptions are much easier to obtain than fixed lines. According to the Telecom Regulatory Authority of India (TRAI), mobile subscribers exceeded fixed line subscribers in 2004, and in December 2005 there were 75.9 million mobile subscribers compared to 48.9 million fixed line subscribers. In China, 61% of mobile service subscribers used data services in 2005, and 3G subscribers are expected to reach 130 million in 2009 (Network and Security Research Institute, 2006). The head of a Chinese mobile carrier reported at a conference that mobile music downloading has surpassed physical music sales in China (*International Herald Tribune*, 15 February 2006). Consumer policy for the mobile commerce market is clearly becoming a global issue.

In order to ensure that the mobile commerce market develops to the benefit of consumers in OECD and non-members, the Committee on Consumer Policy needs to continue to look closely at this issue and evaluate whether existing consumer protection instruments provide adequate protection of consumers. In addition, countries may review their instruments in terms of their consistency with the 1999 *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* ("E-commerce Guidelines"). Member countries' experience indicates a number of possible areas to consider:

- Whether information on contract terms and conditions or complaint procedures is being disclosed effectively to consumers because the limited capacity of the screens on mobile devices may make it impossible to provide all details in a text message.

---

125 According to Dr. Jong-in Lee, Senior Researcher, Korean Consumer Protection Board at the forum session on mobile commerce during the 69th Session of CCP in March 2005.

126 Internet Sweep 2004 by ICPEN (International Consumer Protection Enforcement Network) led by the Norwegian consumer ombudsman, in which 14 countries participated.

- Whether consumers are adequately protected from liability if mobile devices are lost or stolen especially those with a SIM card or contactless/RFID card.

- Whether business practices effectively prevent over-consumption or access to inappropriate services by minors. In particular, it is worth examining whether, if only age verification is provided, it is adequate and whether notices to minors or parents or other measures may be needed.

- Whether businesses implement privacy protection effectively to overcome difficulties in providing relevant information such as privacy policies on the small screen.

- Whether parents as guardians make sure that their children use their mobile phones appropriately.

In addition, in order to improve consumer confidence, businesses involved in mobile commerce may wish to consider the following:

- Whether they are making enough effort to provide appropriate information to consumers on the small screen or by alternative methods.

- Whether they are providing an effective secure payment scheme, including authentication, to prevent unauthorised use, especially in case mobile devices are lost or stolen.[127]

- Whether they allow all consumers to choose to block certain e-mail or sites.

- Whether they (especially carriers, mobile portal site providers and industry organisations) encourage service providers to build sound businesses and to co-operate actively with consumer law enforcement authorities to prevent fraudulent and deceptive practices.

- Whether they disclose their privacy policy effectively and follow the policy to respect the privacy of consumers in a manner consistent with privacy regulation.

- Whether they (especially carriers, financial service providers and industry organisations) encourage improving the security of technologies used in mobile handsets to prevent fraudulent and deceptive practices.

The E-commerce Guidelines apply to business-to-consumer electronic commerce. As they were issued before the development of mobile services, the question arises as to their adequacy for protecting consumers in this new environment. Now that the value of the mobile services market has reached a significant level, further work may be needed at the policy level to address the important consumer issues raised by mobile commerce and the impact they may have on consumer trust in order to ensure that the mobile commerce marketplace reaches its potential.

[127] Only if a handset is a prepaid device and it does not have prepaid card function, it is not necessarily for this concern.

ANNEX A
PROVISION OF COMMERCIAL 3G SERVICES IN OECD COUNTRIES
(AS OF SEPTEMBER 2006)

	Status of 3G services
Australia	Hutchison 3G (3 Australia) started service in April 2003. Telstra started cdma2000 1X services for business customers in December 2002 and services for individuals in September 2005. Vodafone Australia started services in October 2005. Optus started services in November 2005. Telstra and Vodafone Australia launched HSDPA services in October 2006.
Austria	Mobilkom Austria followed One in September 2002 for the technical launch of networks, and in April 2003 started commercial services. Hutchison 3G (3 Austria) started services in May 2003. One started services in December 2003. T-Mobile started data services in May 2004.
Belgium	Proximus started limited services in April 2004 and services for the general public in September 2005. Mobistar will start HSDPA services in Brussels and Antwerp in the third quarter of 2006.
Canada	Bell Mobility, Telus Mobility, Aliant Mobility and MTS Mobility started cdma2000 1X services in 2002.
Czech Republic	Eurotel started services in December 2005. RadioMobil (renamed T-Mobile Czech Republic a.s. since May 2003) plans to launch services by 2007.
Denmark	Hutchison 3G (3 Denmark) started services in October 2003. TDC mobile started commercial services for businesses in October 2005.
Finland	TeliaSonera Finland started services in certain regions in January 2003 and pre-commercial operation in December 2003. Elisa started service in November 2004. DNA Finland also started services in December 2005.
France	SFR started services in June 2004. Orange started trial services in February 2004 and commercial services in December 2004.
Germany	T-Mobile started testing services in February 2002, and its commercial launch started in May 2004. Vodafone Germany started services in May 2004. O2 started services in June 2004. E-Plus Mobilfunk started consumer services in August 2004.
Greece	Teleset started services in February 2004. Vodafone-Panafon started services in November 2004.
Hungary	T-Mobile Hungary started services in Budapest in August 2005. Pannon started services in Budapest in October 2005. Vodafone Hungary started full 3G services in June 2006.
Iceland	No commercial service has been launched.
Ireland	Vodafone started commercial services in July 2004. O2 started limited services in selected markets in December 2003.
Italy	Hutchison 3G Italy launched commercial services in March 2003. TIM and Vodafone Italy started services in May 2004.
Japan	NTT DoCoMo started services in October 2001 with testing services in May 2001. SOFTBANK MOBILE Corp. (formerly Vodafone Japan and, at that time, known as J-Phone) started services in December 2002 after testing services in June 2002. KDDI started services using cdma2000 1X in April 2002 and launched services using cdma2000 1X EV-DO in November 2003.
Korea	LG Telecom started services nationwide in 2001. SK Telecom started services in February 2002. KTF started services in June 2003. While both companies have used cdma2000 technology, they also started W-CDMA services in December 2003.
Luxembourg	Tele2 started services in May 2003. P&T Luxembourg started services in June 2003.

	Status of 3G services
Mexico	Grupo Iusacell started services using cdma2000 1X in January 2003.
Netherlands	KPN Mobile started services in July 2004. Vodafone Netherlands started services in June 2004.
New Zealand	New Zealand Telecom started cdma2000 1X services in July 2002 and upgraded to 1XEX-DO in November 2004. Vodafone New Zealand started services in August 2005.
Norway	Telenor started services in December 2004. NetCom started services in March 2005.
Poland	Sferia started cdma2000 1X services in November 2002. The launch date of other operators was postponed. Among these, PTC launched business services in April 2005.
Portugal	Vodafone Portugal started limited services in selected markets in January 2004. TMN started services in April 2004. Optimus started services in June 2004.
Slovak Republic	T-mobile Slovakia started services in Bratislava in January 2006. Orange Slovensko started services in August 2006.
Spain	All 3G operators set a UMTS system for technical trials before June 2002. Telefonica Moviles and Vodafone started services in May 2004.
Sweden	Hutchison 3G (3 Sweden) started services in May 2003. TeliaSonea started services in March 2004. Tele2 started services in June 2004.
Switzerland	Swisscom started 3G services in September 2004. Orange Switzerland started services in September 2005. Sunrise started services in December 2005.
Turkey	No commercial service has been launched.
United Kingdom	Hutchison 3G (3 UK) started services in March 2003. T-Mobile started data-only 3G services in February 2004. Vodafone started services in March 2004 and Orange started services in December 2004. O2 started business services in October 2004 and consumer services in February 2005.
United States	Several operators announced the provision of nationwide 3G services including Verizon Wireless, which started cdma2000 Ix EV-DO services in certain regions in September 2003. Cingular AT&T Wireless (now Cingular Wireless) started services in July 2004. Sprint Nextel started cdma2000 Ix EV-DO services in July 2005. T-Mobile USA expects to start services by the end of 2006.

Note: "Services" do not always mean "consumer services".

Source: OECD (2004), "Development of Third-Generation Mobile Services in the OECD", September, Table 8, updated with information from UMTS Forum, CDMA Development Group and individual carriers.

ANNEX B
INTERNATIONAL ORGANISATIONS FOR MOBILE COMMERCE

CDMA Development Group (CDG)

The CDMA Development Group (CDG) was founded in December 1993. It is an international consortium of companies which have joined together to lead the adoption and evolution of 3G CDMA wireless systems around the world. The CDG is comprised of CDMA service providers and manufacturers, application developers and content providers. By working together, the members help to ensure interoperability among systems, while expediting the availability of 3G CDMA technology to consumers.

GSM Association (GSMA)

The GSM Association was founded in 1987 by 15 operators committed to the joint development of a cross-border digital system for mobile communications. It is a global trade association which seeks to promote, protect and enhance the interests of GSM mobile operators worldwide. It deals not only with mobile commerce issues such as those related to spectrum and roaming but also with fraud against networks and security concerns.

At the end of July 2006, its members were 699 mobile operators and 185 GSM manufacturers and suppliers. Current board members are from Hutchison Whampoa Group (Hong Kong, China), Turkcell Iletisim Hizmetleri (Turkey), Bharti (India), Rogers Communications (Canada), Telefónica Móviles (Spain), Singapore Telecommunications, Telenor Mobile (Norway), SFR (France), Vodafone (United Kingdom), Orange (France), Smart (Philippines), China Mobile (China), TeliaSonera (Sweden), Cingular Wireless (United States), KTF (Korea), Orascom Telecom (Egypt), VimpelCom (Russia), China United Telecommunications (China), and NTT DoCoMo (Japan) as well as T-Mobile International, TIM.

Mobey Forum

The Mobey Forum was founded in May 2000 by a number of the world's leading financial institutions and mobile terminal manufacturers (ABN-AMRO Bank, HSBC, Nokia, Nordea and UBS) with the mission of encouraging the use of mobile technology in financial services.

Ever since its establishment, the Forum has consistently worked towards this goal. One of its major achievements was the announcement of the Preferred Payment Architecture in June 2001, with extensive documentation defining both the business and technical aspects of providing user-friendly and secure mobile banking and payment services. In September 2002, the Forum published Preferred Payment Architecture for Local Payments and demonstrated local mobile transactions.

Based on the Preferred Payment Architecture principles, the Forum published a White Paper on Mobile Financial Services in June 2003. The White Paper looks at mobile financial services in the current and changed technology environment. In 2005, the Forum issued key findings from technical analysis as security elements of mobile devices.

Mobile Electronic Transactions (MeT)

The MeT was formed in 2000 by major mobile phone manufacturers. Since its establishment, MeT has slightly changed its focus. In the early years, it focused on the development of technical specifications for remote transactions and on closer collaboration between players in the handset industry. Later, the focus has evolved towards proximity transactions such as local payments, mass transit ticketing and advertising enabled by Near Field Communication. From the beginning of 2005, MeT and its members have participated in the NFC Forum in order to include key usability, security and interoperability requirements in the group for technical specification. Members are Ericsson, Nokia, NEC and Panasonic.

Mobile Entertainment Forum (MEF)

The MEF is a global trade association representing participants in the mobile entertainment value chain interested in driving the industry's evolution and commercial potential through collaboration, consultation and promotional activities. It was founded in February 2001 by six leading players (Booz-Allen & Hamilton, Cash-U, Comverse, mBlox, OpenMobile and Picofun). It is committed to reducing the barriers to entry into the innovative mobile entertainment market, thereby encouraging entry by new businesses and increasing competition and growth to the benefit of all industry players and consumers. Its objectives are *i)* advocacy and outreach, *ii)* awareness building, and *iii)* setting guidelines. Current board members are from Amobee, mBlox, Eyeka, Sony BMG, Denton Wilde Sapte, Alcatel, Vodafone, EMI Music, France Telecom, Beep Science, and Sun Microsystems.

Mobile Payment Forum

The Forum is a global, cross-industry organisation launched in November 2001 to create a framework for the deployment of simple, secure and interoperable m-payments. The Forum provides an open, flexible and trusted environment in which member organisations can clarify opportunities and address the complex challenges facing the industry.

Members of the Forum includes organisations involved in facilitating mobile payments: key financial institutions, payment card companies, telecommunications operators, wireless-device manufacturers, merchants, content providers and software and hardware developers and vendors.

Its mission is to leverage the expertise of key participants in the mobile communications and financial industries to create a foundation for standardised technology and functionality for mobile payments, thereby addressing consumer and merchant needs for simple, secure and interoperable m-payment choices. The Forum is now working on mobile payment configuration, guidelines for mobile payment authentication and secure and interoperable infrastructure for payment processing. Current board members are VISA international, MasterCard International, Nokia, Vodafone, Telecom Italia Mobile, Sprint, First Data International.

OMA (Open Mobile Alliance)

According to the OMA, the alliance was formed in June 2002 by nearly 200 companies, including the world’s leading mobile operators, device and network suppliers, information technology companies and content and service providers. The fact that the whole value chain is represented in OMA marks a change in the way specifications for mobile services are done. Rather than keeping the traditional approach of organising activities around “technology silos”, with different standards and specifications bodies representing different mobile technologies working independently, OMA aims to consolidate in one organisation all specification activities in the service-enabler space.

OMA is the focal point for the development of mobile service enabler specifications, which support the creation of interoperable end-to-end mobile services. It drives service enabler architectures and open enabler interfaces that are independent of the underlying wireless networks and platforms. It creates interoperable mobile data service enablers that work across devices, service providers, operators, networks and geographies. It issued version 2.0 of Interoperable DRM in April 2006. OMA will develop test specifications, encourage third-party tool development and conduct test activities that allow vendors to test their implementations.

A year into the formation of OMA, significant consolidation had been achieved with the integration into OMA of the WAP Forum, Location Interoperability Forum (LIF), SyncML Initiative, MMS-IOP (Multimedia Messaging Interoperability Process), Wireless Village, Mobile Gaming Interoperability Forum (MGIF), and the Mobile Wireless Internet Forum (MWIF). This consolidation promotes end-to-end interoperability across different devices, geographies, service providers, operators and networks, and further supports OMA's market and user requirements focus to guide specification work.

The goals of the OMA

1. Deliver high-quality, open technical specifications based upon market requirements that drive modularity, extensibility and consistency among enablers to reduce industry implementation efforts.

2. Ensure that OMA service enabler specifications provide interoperability across different devices, geographies, service providers, operators and networks and facilitate interoperability of the resulting product implementations.

3. Be the catalyst for the consolidation of standards activity within the mobile data service industry, working in conjunction with other standards organisations and industry forums to improve interoperability and decrease operational costs for all involved.

4. Provide value and benefits to members in OMA from all parts of the value chain including content and service providers, information technology providers, mobile operators and wireless vendors such that they elect to actively participate in the organisation.

ANNEX C
CONSUMER PROTECTION LAWS ON MOBILE COMMERCE

	General protection	Unsolicited sale	Disclosure	Unauthorised use	Parental consent	Excessive consumption	Inappropriate services
Australia	Trade Practices Act 1974, Telecommunications Act 1997	Trade Practices Act 1974	Trade Practices Act 1974	×	State and territory law	Credit Management Code, Telephone Information Services Standards Council (TISSC) Code of Practice	Telecommunications Act 1997, Telecommunications (Consumer Protection and Service Standards) Act 1999, Broadcasting Services Act 1992, Classification (publications, Films and Computer Games) Act 1995, Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No. 1) , Criminal Code Act 1995
Austria	Civil Code, Law on Unfair Competition, E-commerce law, law on distance selling		×	×	Civil Code	×	×
Belgium	Act of 14 July 1991 on trade practices and consumer information and protection (LPC), Act of 17 July 2002 concerning transactions carried out by electronic transfer of funds, Act of 11 March 2003 on certain legal aspects of information society services, Act of 12 May 2003 on the legal protection of services based on conditional access and services concerning information society services	Art. 76 in LPC	×	×	Art. 1124 of the Civil Code	Art. 1384 of the Civil Code	×
Canada	Competition Act and provincial and territorial legislation, Internet Sales Contract Harmonization Template (May 2001)		×	×			Consumer Protection Act (Quebec), sec. 248
Czech Republic	Civil Code, Consumer Protection Act, Act on Electronic Communications		×	×	Civil Code (Para. 9)	Act on Electronic Communications (Para. 44)	Act on Electronic Communications, para. 44
Denmark	Danish Contracts Act	×	×	Act on Certain Payment Instruments, Sec. 11	Danish Guardianship Act		Framework agreement for mobile content services (Telecommunication Industries Association)

	General protection	Unsolicited sale	Disclosure	Unauthorised use	Parental consent	Excessive consumption	Inappropriate services
Finland	Consumer Protection Act (CPA), Act on the Provision of Information Society Services, Act on the Protection of Privacy in Electronic Communications	CPA, Ch. 2 (regulation of marketing) and Ch. 7 (direct marketing) of PPA	CPA, Ch. 6 sec, 13, Act on the Provision of Information Society Services	Communications Market Act, sec. 76, a new proposal by a working group	The Guardianship Services Act sec. 23, 24 etc Case between the Habbo-Hotel Kultakala Internet service and CO		CPA, Ch. 2 sec. 1, Ch. 3, sec. 1, Consumer Ombudsman's Guidelines (Minors, marketing and purchases), Public Order Act, Act on classification of audiovisual programmes, Ch. 2, sec. 3
Germany	General (consumer) contract law of the Civil Code (BGB), Telecommunications Act (TKG) (abusive use of telephone number)	×	BGB, sec. 312b-312e	×	BGB, sec. 104-113 of	BGB, sec. 1626 subsection 1 of	StGB, sec. 184, 184c
Hungary	Civil Code, Consumer Protection Act, Decree on distance contracts, Decree on inner commerce	×	×	×	Civil Code		
Japan	Consumer Contract Act, Act against Unjustifiable Premiums and Misleading Representations, Specified Commercial Transactions Law	Specified Commercial Transactions Law	×	×	Civil Code, art. 5	×	×
Korea	Electronic Commerce Act, Electronic Signature Act, Electronic Transactions Act, Act on Consumer Protection in Electronic Commerce (CPEC), and Guidelines for Consumer Protection in Electronic Commerce, Location-based Information Use and Protection Act	CPEC, art. 21	×	×	Act on Protection of Information and Promotion of Information Communication Network	Civil Act, CPEC art. 13-3	Act on Protection of Information and Promotion of Information Communication Network, Youth Protection Act
Mexico	Federal Law of Consumer Protection (LFPC), Chapter VIII bis	LFPC, art. 76bis, 10, 86bis	×	LFPC, art. 76bis and 86bis	Federal Civil Code, art. 1795 and art. 23	Civil Code, art.1919	Cybernetic Police, FLCP, art. 76bis, Law for protecting Rights Of Girls, Boys And Teenagers
Norway	Marketing Control Act (MCA), Guardianship Act, Act relating to information requirements and right of withdrawal, Lottery Act, Personal Data Act, CO Guidelines on Mobile Content Services.	MCA, sec. 2a of the	×	×	Guardianship Act, sec. 2	CO guidelines Ch. 2.1, 5.4, 5.5, 5.2; Personal Data Act	CO guidelines, 4.1, 4.2
Poland	Civil Code, Telecommunications Law, Act on providing services by electronic communications	×	×	×	Civil Code	×	×

	General protection	Unsolicited sale	Disclosure	Unauthorised use	Parental consent	Excessive consumption	Inappropriate services
Slovak Republic	Act No. 634/1992 Coll. on Consumer Protection (sale of goods), Act No. 22/2004 Coll. on Electronic Commerce, Act No. 108/2000 Coll. on Consumer Protection in Door-to-door and Mail Order Sales, Act No. 147/2001 Coll. on Advertising, Act No. 610/2003 Coll. on Electronic Communication		Act No.108/2004 Coll. On Electronic Commerce, 10(1), 10(4)	×	Civil Code, sec. 8	Civil Code	Criminal Act No 300/2005 Coll (protection of minors)
Switzerland	Civil Code (Droit des obligations)		×	×	Civil Code, art. 19	Civil Code	Penal Code, art. 197
Sweden	Consumer Sales Act, Consumer Services Act, Distant Sales and Door to Door Sales Act	Swedish Marketing Act, sec 6	Distant Sales and Door to Door Sales Act, Ch. 2, sec. 6	Act on Electronic Communication, Consumer Credit Act	Children and Parents Code, Ch. 9	Distant Sales and Door to Door Sales Act	×
United Kingdom	Distance Selling Regulations		×	Government works with industry		Advertising Standards Authority, Advertising Codes	Government works with industry
United States	FTC Act, Telephone Consumer Protection Act (TCPA)		FTC Act, Dot Com Disclosures Guidance	×	State Law	×	Children's Online Privacy Protection Act
European Commission	Distance Selling Directive 97/7/EC	Unfair Commercial Practices Directive (2005/29/EC)	×		×	Opinion of Article 29 Working Group	Safer Internet Forum

Note: This table is based on responses from member countries. "×" indicates that there are no provisions to address specific problems consumers may have with mobile commerce.

ANNEX D
OECD STUDY ON MOBILE CONTENT (OECD, 2005C)

Demand for mobile content and role of user preferences in successful development of mobile content

While still a relatively new field, mobile content is viewed as a major driver of growth for the telecommunications and media industries.

Mobile content – particularly music and games – is viewed as an emerging major industry. Markets are most developed in Asia, with very large growth potential in North America and Europe.

Ease of use and personalisation are essential to broad user uptake of mobile content.

As mobile content markets develop, numerous players are vying to control various parts of a complex and changing value chain. These include content owners and developers, content aggregators, mobile operators, handset manufacturers and various other companies offering enabling technologies. No single dominant value chain has emerged and it is likely that different value chains will prevail for different types of mobile content, reflecting the differing nature of the industries involved, different market structures and competitive conditions, and the different policy frameworks that apply to different types of content.

Key technologies required to enable broadband mobile content

Broadband wireless networks, particularly 3G, will provide the bandwidth necessary to deliver increasingly sophisticated mobile content. Earlier generation wireless networks have seen increasing customer demand for content such as ringtones, music downloads and simple games. As providers increase network bandwidth, the opportunities for mobile content will expand.

Handset manufacturers are working with content developers, mobile operators and other industry participants to develop handsets and features that will facilitate access to and use of mobile content. To complement these initiatives, industry and government must facilitate the development of standards and interoperability guidelines.

Technologies crucial to enabling broad content dissemination, including marketing, distribution and billing technologies, are increasingly available and will encourage further development of mobile content. Mobile portals provide many of these capabilities and occupy a primary position in the mobile content value chain. Currently, most users obtain content on mobile devices from their mobile operator through the operators' branded mobile portal that provides content from providers with whom the mobile operator has an established relationship. As new technologies are introduced, this position could change.

Pricing of mobile content can be confusing for some customers. A lack of pricing information can leave customers unsure of the cost of acquiring or using content, due in part to data transfer costs.

As with online content, piracy, IP rights and digital rights management issues are being addressed by the mobile content industry. It is essential that as these policies develop globally, consideration is given to mobile platforms.

Mobile content offerings

While many possibilities exist for generating attractive mobile content, to date music – especially ringtones and most recently music downloads - is a key source of mobile content. Growth in the mobile music markets involves song reproductions or snippets that do not raise as much industry concern over copying. As offerings become more full track-oriented, however, these concerns will probably be of increasing prominence.

Games are also a key focus of many mobile content developers, and increasingly, games are being developed for mobile platforms. To date, the market has focussed on fairly simple embedded games, but there is a growing market for more complex, interactive and multiplayer mobile games. Industry standards and interfaces would greatly enhance development of mobile games by allowing developers to address a broader market. As more sophisticated games are developed, the software can potentially be adapted for enterprise training and educational purposes.

A variety of other content is being provided over mobile platforms, including video, enterprise and information and location services. Some of this content, including adult and gambling, raise unique policy issues that are not general to other types of mobile content. Location-based services also raise privacy concerns.

Policy issues

Because broadband wireless deployment is crucial to further advances in mobile content, infrastructure policies, including broadband, wireless and spectrum policies, are essential to ensure that network developments keeps pace with the content being transmitted over them.

Numerous R&D projects are designed to facilitate the development of mobile content. These, along with public-sector use of mobile content applications, can forge new business models and promote user acceptance.

IP, DRM and technical standards are essential to continued growth. Industry and government-facilitated policies to encourage consensus and development in these areas must take into account the mobile environment.

Competition is essential to ensure that industry participants do not foreclose mobile content from new technological platforms.

Mobile platforms raise issues of privacy, security and consumer protection that must be addressed by ongoing policy initiatives.

Payment and micro-payment policies should specifically consider the mobile content markets.

As content flows globally, taxation policies should consider the significant impact they can have on the uptake of mobile content.

BIBLIOGRAPHY

Ackerman, L. *et al*. (2003) "Wireless Location Privacy: A Report on Law and Policy in the United States, the European Union and Japan", www.docomolabs-usa.com/pdf/DCL-TR2003-001.pdf.

Ahmad, N.Z.B. *et al*. (2004), "A Distributed Geographical Location Information System with Flexible Privacy and Security Enhancement Function", Information Processing Society of Japan SIG-MBL, No.95, pp. 25-32, September (in Japanese).

Association Française des Opérateurs Mobiles (AFOM) and TNS Sofres (2005), *Observatoire sociétal du téléphone mobile,* Première édition, Paris.

ATLAS Research Group and Info-Sharing Business Institute (2006), *Current Condition and Issues of WiBro Business in Korea*, August.

Australian Interactive Media Industry Association (2006), *Australian Mobile Phone Lifestyle Index*, 2nd edition, May.

AlShaali, S. and U. Varshney (2005), "On the usability of mobile commerce", *International Journal of Mobile Communications*, Vol. 3(1), pp. 29-37.

Arthur D. Little (2004), *Global M-Payment Report 2004*, Vienna, Austria.

A.T. Kearney and Judge Institute of Management Studies (2004), *Mobinet Index 2004*, July.

A.T. Kearney and Judge Institute of Management Studies (2005), *Mobinet Index 2005*, October.

Australian Communications and Media Authority (2005), *Telecommunications Performance Report 2004-05*, November.

Bank of Korea (2004), "Domestic Internet Financial Service Trends in September 2004", October (in Hangul).

Bank of Korea (2005), "Domestic Internet Financial Service Trends in June 2005", July (in Hangul).

Bank of Korea (2006a), "Domestic Internet Financial Service Trends in 2005", February (in Hangul).

Bank of Korea (2006b), "Domestic Internet Financial Service Trends in June 2006", August (in Hangul).

Banksys (2006), *Annual Report 2005*, Brussels.

Barnes, S.J. (2002), "The Mobile Commerce Value Chain: Analysis and Future Developments", *International Journal of Information Management* 22, pp.91-108.

Bluetooth SIG (2006a), "What can consumers do to protect their data?", www.bluetooth.com/Bluetooth/Learn/Security/.

Bluetooth SIG, (2006), **"**What are phone manufacturers doing to address the situation?", www.bluetooth.com/Bluetooth/Learn/Security.

Bruner II, G.C. and A. Kumar (2005), "Explaining Consumer Acceptance of Handheld Internet Devices", *Journal of Business Research*, Vol. 58, issue 5, pp. 553-558.

Buellingen, F. and M. Woerter (2004), "Development Perspectives, Firm Strategies and Applications in Mobile Commerce", *Journal of Business Research*, vol. 57, issue 12, pp. 1402-1408.

Cabinet Office (2006), "The Survey of Consumers' Opinion on Mobile Phones and Mobile Commerce", Fourth Survey of Quality-Life monitors in FY2006, Japan (in Japanese).

Chang, Y.F. and C.S. Chen (2005), "Smart phone – the choice of client platform for mobile commerce", *Computer Standards & Interfaces*, 27 (2005) pp. 329-336.

Chou, Y. *et al.* (2002), "Understanding M-commerce Payment Systems through the Analytic Hierarchy Process", *Journal of Business Research* 5802.

Consumer Affairs Victoria (2002), *M-Commerce: What is it? What will it mean for consumers?*, Sydney, Australia.

Consumer Affairs Victoria (2004), *Considering the implications of m-commerce – A Consumer Perspective*, Sydney, Australia.

Cousins, C. (2005) "Threats on Mobile Devices" ASEM Cyber Security Workshop, Seoul.

Deloitte Touche Tohmatsu (2006), *TMT Trends: Predictions, 2006*, January.

Department of Communications, Information Technology and the Arts of Australia (DCITA) (2006), *Review of the Regulation of Content Delivered over Convergent Devices*, April. www.dcita.gov.au/__data/assets/pdf_file/39890/Final_Convergent_Devices_Report.pdf.

Dholakia, R.R. and N. Dholakia (2002), "Mobility and Markets: Emerging Outlines of M-commerce", *Journal of Business Research* 5828.

Electronic Commerce Promotion Council of Japan (ECOM) (2004a), *Security Guidelines for Mobile EC*, Tokyo (in Japanese).

ECOM (2004b), *Survey for Mobile Internet Use*, Tokyo (in Japanese).

ECOM (2005), *Survey for Mobile Internet Use*, Tokyo (in Japanese).

European Commission (2002), *Digital Content for Global Mobile Services*, Luxembourg.

E-Japan Forum (2005), *The Guide for Safe Internet Life*, Tokyo (in Japanese).

EC Article 29 Working Party (EC Working Party on the Protection of Individuals with Regard to the Processing of Personal Data) (2005), *Opinion on the use of location data with a view to providing value added services*, WP 115, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

Evers, Joris (n.d.), "Is your cell phone due for an antivirus shot?", news.zdnet.com/2100-1009_22-6042745.html.

Federal Communications Commission (2002), *In the Matter of the request by the Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Information Practices*, WT Docket No. 01-72, FCC 02-208, hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-208A1.doc

Frost and Sullivan (2006), *Latin American Mobile Content Services Markets*, July.

F-Secure (2006), "Austrian Operator ONE offers exclusive antivirus mobile protection with F-Secure", press release, 31 May, www.f-secure.com/news/items/news_2006053100.shtml.

Gajparia, A. *et al.* (2004), "The Location Information Preference Authority: Supporting user privacy in location based services", in S. Liimatainen and T. Virtanen (eds.), Nordsec 2004, The 9th Nordic Workshop on Secure IT-systems, Helsinki University of Technology, Finland, November, pp. 91-96.

Gu, T. *et al.* (2005), "Towards a Flexible Service Discovery", *Journal of Network and Computer Applications*, Vol. 28, Issue 3, August, pp. 233-248 .

Guan, S., C.S. Ngoo, and F. Zhu (2004), "Handy Broker: An Intelligent Product Brokering Agent for M-commerce Applications with User Preference Tracking", *Electronic Commerce Research and Applications* 1, pp. 314-330.

Handschuch, H., (2004), "Contactless Technology Security Issues", *Information Security Bulletin*, Vol. 9, pp. 95-100.

Heiden, H. (2005), "Mobile decision support for in-store purchase decisions", *Decision Support Systems*, forthcoming.

Hicks, S. (2006) "Best Practices for securing mobile devices", searchmobilecomputing.techtarget.com/generic/0,295582,sid40_gci1163542,00.html.

IBM (2005), *2004 Global Business Security Index Report,* www-935.ibm.com/services/us/index.wss/summary/imc/a1008866.

IBM (2006), *2005 Global Business Security Index Report*, www-03.ibm.com/press/us/en/pressrelease/19141.wss.

iGillott Research (2005), *Mobile Content Enablers: Boosting Mobile Operator Profitability*, August.

Internet Association Japan (IAJ) (2003), *Children, Mobile Phones and the Internet: the Mobile Internet and Children*, The Experts' meeting, 6-7 March, Tokyo, Japan.

International Working Group on Data Protection in Telecommunications (2004), Common Position on Privacy and Location Information in Mobile Communications Services, www.berlin.de/Datenschutz/doc/int/iwgdpt/local_neu_en.pdf.

Itani, W. and A. Kayssi (2004), "J2ME Application Layer End-to-End Security for M-commerce", *Journal of Network and Computer Applications* 27, pp. 13-32.

Impaq Group (2005), *Mobile Life 1: Challenging the Rules of Loyalty*, April.

Ipsos Insight (2006), *Little Internet Fact Guide 2006*, July.

In-Stat (2006), *Mobile Wallet: More than M-Commerce*, April.

Jyrkönen, J and H. Paunonen (2003), "Card, Internet, and mobile payments in Finland", Bank of Finland Discussion Papers, 8-2003, March.

Juniper Research (2004), *Mobile Commerce & Micropayment Strategies*, Newbury, United Kingdom.

Juniper Research (2006a), *Mobile TV: Watch it Grow*, Second Edition, July 2006, Newbury, United Kingdom.

Juniper Research (2006b), *Mobile Data Protection*, September 2006, Newbury, United Kingdom.

Karygiannis, T. and L. Owens (2002) "Wireless Network Security, Bluetooth and Handheld Devices" NIST Special Publication 800-48.

Kishida, S. (2003), "New Global Trend of Mobile Commerce", *Info Com Review*, Vol. 30, pp. 19-28 (in Japanese).

Korean Consumer Protection Board (2002), *Consumer Protection in Mobile Commerce*, May.

Korea National Statistical Office (2005), *E-commerce in 2004 and in the Fourth Quarter 2004*, April.

Korea National Statistical Office (2006), *Cyber Shopping Mall Survey in December and in 2005*, February.

Kumar, S. and C. Zahn (2003), "Mobile Communications: Evolution and Impact on Business Operations", *Technovation* 23, pp. 515-520.

Laforet, S. and X. Li, (2005), "Consumers' attitudes towards online and mobile banking in China", *International Journal of Bank Marketing*, Vol. 23 No. 5, pp. 362-380.

Laurie, A., B. Laurie and A.L. Digital Ltd. (2004), "Security Briefs, Bluetooth", www.thebunker.net/security/bluetooth.htm.

Lin, H.H. and Y.S. Wang (2006), "An Examination of the Determinants of Customer Loyalty in Mobile Commerce Contexts, Information and Management", *Information & Management*, Vol. 43, Issue 3, pp. 271-282.

Luarn, P. and H.H. Lin (2005), "Toward an Understanding of the Behavioural Intention to Use Mobile Banking", *Computers in Human Behaviour*, Vol. 21, Issue 6, pp. 873-891.

Mathatanankoon, P. *et al.* (2005), "Consumer-based M-Commerce: Exploring Consumer Perception of Mobile Applications", *Computer Standards & Interfaces*, 27, pp. 347-357.

McDowell, M. and M. Lytle (2005) "Understanding Bluetooth Technology", www.us-cert.gov/cas/tips/ST05-015.html.

Media Awareness Network (2005), *Young Canadians in a Wired World Phase II – Trends and Recommendations*, November.

Ministry of Economy, Industry, and Trade of Japan (METI) (2006), *The E-Commerce Guidelines*, Tokyo, www.meti.go.jp/press/20060201002/junsoku,kaitei-set.pdf.

Ministry of Internal Affairs and Telecommunication of Japan (MIC) (2004), *Information and Telecommunication in Japan 2004 -Building a Ubiquitous Network Society That Spreads Throughout the World*, Tokyo.

MIC (2005), *Information and Telecommunication in Japan 2005 - Stirrings of u-Japan*, Tokyo.

MIC (2006*), Information and Telecommunication in Japan 2006 - Ubiquitous Economy*, Tokyo.

Ministry of Transport and Communications Finland (2005), *Mobiilipalvelumarkkinat Suomessa 2004* (Mobile Services Market in Finland 2004), 34/2005 (in Finnish).

Mitsubishi Research Institute (2006), *Usage of Mobile Phones by Minors*, March (in Japanese).

Mitsubishi Research Institute and Rakuten, Inc. (2003a), *First Survey of Users for Mobile Contents / Services*, September (in Japanese).

Mitsubishi Research Institute and Rakuten, Inc. (2003b), *Fourth Survey of Users for Mobile Contents / Services*, December (in Japanese).

Mitsubishi Research Institute and Rakuten, Inc. (2004), *Tenth Survey of Users for Mobile Contents / Services*, July (in Japanese).

Mitsubishi Research Institute and Rakuten, Inc. (2005a), *Fourteenth Survey of Users for Mobile Contents / Services*, February (in Japanese).

Mitsubishi Research Institute and Rakuten, Inc. (2005b), *Sixteenth Survey of Users for Mobile Contents / Services*, May (in Japanese).

Mitsubishi Research Institute and Rakuten, Inc. (2006), *Twentieth Survey of Users for Mobile Contents / Services*, March (in Japanese).

Morioka, T. (2003), "Possibility of Mobile Phones with Mobile Commerce", *Creation of Intellectual Assets*, September, pp. 89-91 (in Japanese).

Mort, G.S. and J. Drennan (2004), "Marketing M-services: Establishing a Usage Benefit Typology Related to Mobile User Characteristics", *Database Marketing & Customer Strategy Management*, Vol. 12, 4, pp. 327-341.

Nakanishi, K. *et al.* (2003), "LEXP: Preserving User Privacy and Certifying the Location Information," Information Processing Society of Japan, the 2nd Workshop on Security at the Ubicomp 2003 Conference.

National Congress of Parents and Teachers Association of Japan (2005), *Survey on the Youth and Internet and other media*, May (in Japanese).

The National Consumer Affairs Center of Japan (2006), *Troubles on the mobile phones which can be used abroad*, January (in Japanese).

National Internet Development Agency of Korea (2006), *2006 Korea Internet White Paper*, Seoul.

Naruse, K. (2002), "What Mobile Commerce Users Seek Next?" *Study on Security*, October, pp. 30-32 (in Japanese) .

Network and Security Research Institute (2006), *Mobile Phone Market in China*, March (in Japanese).

Ngai, E.W.T. and A. Gunasekaran (2005), "A Review for Mobile Commerce Research and Applications", *Decision Support System*, forthcoming.

Nikkei BP (2005), *Information Protection in Mobile Devices*, April, http://itpro.nikkeibp.co.jp/article/KEITAI/20051004/222205/ (in Japanese).

Nokia (2005) "Protect Mobile Devices and Networks", europe.nokia.com/nokia/0,,75960,00.html.

NTT DoCoMo (2004), "What i-mode Changes", *NTT DoCoMo Report*, February (in Japanese).

New South Wales Office of Fair Trading, Australia (2003), *Youth Debt*, November.

OECD (2001), "Report on Consumer Protections for Payment Cardholders", DSTI/CP(2001)3/FINAL, OECD, Paris.

OECD (2004a), "Developments of Third-Generation Mobile Services in the OECD", DSTI/ICCP/TISP (2003)10/FINAL, OECD, Paris.

OECD (2004b), "Consumer Protection in Mobile Commerce of Korea", internal working document, OECD, Paris.

OECD (2004c), "Consumer Protection in Mobile Commerce (note by Finland)", internal working document, OECD, Paris.

OECD (2005a), "Background Report on Consumer Dispute Resolution and Redress in the Global Marketplace", DSTI/CP(2004)6/FINAL, OECD, Paris.

OECD (2005b), "The Implication of WiMax for competition and regulation", DSTI/ICCP/TISP(2005)4/FINAL, OECD, Paris.

OECD (2005c), "Digital Broadband Content: Mobile Content", DSTI/ICCP/IE(2004)14/FINAL, OECD, Paris.

OECD (2005d), "Digital Broadband Content: Music", DSTI/ICCP/IE(2004)12/FINAL, OECD, Paris.

OECD (2005e), "Digital Broadband Content: The online computer and video game industry", DSTI/ICCP/IE(2004)13/FINAL, OECD, Paris.

OECD (2005f), "Guide to Measuring the Information Society", DSTI/ICCP/IIS(2005)6/FINAL, OECD, Paris.

OECD (2005g), "Consumer Complaints and Policy Issues related to Mobile Commerce in Korea", internal working doc, OECD, Paris.OECD (2006), "Digital Broadband Content: Digital Content Strategies and Policies", DSTI/ICCP/IE(2005)3/FINAL, OECD, Paris.

Pescatore, J. and J. Girard (2005) "Fast Spreading Virus or Worm Won't Affect Mobile Devices Before Year-End 2007", Gartner Report, www.gartner.com/DisplayDocument?doc_cd=127808.

Pew Internet & American Life Project (2006a), "How Americans Use Their Cell Phones", April.

Pew Internet & American Life Project (2006b), "The Future of Internet II", September.

Piloura, T. *et a.l* (2005), "Using Web Services for Supporting the Users of Wireless Devices", *Decision Support Systems*, forthcoming.

Portio Research (2006a), *MoCo Technology Guide 2006*, May.

Portio Research (2006b), *Multimedia Mobile Entertainment Futures 2006-2010*, September.

Rawson, S. (2002), "E-Commerce – Mobile Transactions", *Computer Law & Security Report*, Vol. 18(3), pp. 164-171.

Rettie, R. *et al.* (2005), "Text Message Advertising: Response Rates and Branding Effects", *Journal of Targeting, Measurement and Analysis for Marketing*, Vol. 13 No. 4, pp. 304-312.

Rockbridge Associates and Robert H. Smith School of Business at the University of Maryland (2006), 2005/2006 National Technology Readiness Survey, Collage Park, Maryland, July.

Sawai, K. *et al.* (2002), "Standardization for Mobile Commerce", *NTT Technology Journal*, January, pp. 31-34 (in Japanese).

Scornavacca, E. Jr. and S.J. Barnes, "Barcode Enabled M-commerce: Strategic Implications and Business Models", *International Journal of Mobile Communications,* Vol. 4 (2), pp. 163-177.

Shaked, Y. and A. Wool (2005), "Cracking the Bluetooth PIN", School of Electrical Engineering Systems, Tel Aviv University, www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/.

Strategy Analytics (2006), *Worldwide Cellular User Forecasts, 2005-2010*, January.

Survey Research Center (2005), *Mobile Use by Children*, April, Japan (in Japanese).

Takegami, K. (2003), "Key Technology for Mobile Phones and Futures for Mobile Carriers in 2010", *InfoCom Review*, Vol. 30, pp. 4-18 (in Japanese).

Thanh, D.V. (2000), "Security Issues in Mobile eCommerce", *Lecture Notes in Computer Science*, Vol. 1875, pp. 467-476.

Trans Atlantic Consumer Dialogue (TACT) (2005), *Resolution on Mobile Commerce*, August, www.tacd.org/db_files/files/files-395-filetag.doc.

Trans Atlantic Consumer Dialogue (TACD) (2006), *Report on the July 2006 TACD Mobile Commerce Survey*, September, www.tacd.org/db_files/files/files-413-filetag.pdf.

Trend Micro (2005), *Security for Mobile Devices: Protecting and Preserving Productivity*, November.

United Nations Conference on Trade and Development (UNCTAD) (2005), *Information Economy Report 2005,* New York and Geneva.

Yankee Group (2005), *Global Wireless/Mobile Premium Forecast*, November.

Whitehouse, O. (2003) "War Nibbling: Bluetooth Insecurity", www.rootsecure.net/content/downloads/pdf/atstake_war_nibbling.pdf.

Witteman, M. (2006), "Smart Card Security Testing", 31 March, www.testnet.org/Produktie/Bibliotheek/Presentaties%20voorjaar%202006/Track%201%20-%20Smart%20Card%20Security%20Testing.pdf.

Wu, J.H. and T.L. Hisa (2004), "Analysis of E-commerce Innovation and Impact: A Hypercube Model", *Electronic Commerce Research and Application*, Vol. 3, Issue 4, pp. 389-404.

Wu, J.H. and S.C. Wang (2005), "What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model", *Information & Management*, 42, pp. 719-729.

Zhang, N. *et al.* (2004), "Autonomous Mobile Agent Based Fair Exchange", *Computer Networks*, Vol. 46, Issue 6, pp. 751-770.