ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Directorate for Science, Technology and Industry
Committee for Information, Computer and Communications Policy

OECD Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce

OECD Ministerial Meeting
on the Future of the Internet Economy
Seoul, Korea, 17-18 June 2008
Hosted by 방송통신위원회 KOREA COMMUNICATIONS COMMISSION

OECD Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce

I. Introduction

Mobile commerce developments

For the purposes of this document, mobile commerce, also known as "mobile e-commerce" or "m-commerce," means commercial transactions and communication activities conducted through wireless communication services and networks by means of short message services ("SMS"), multimedia messaging service ("MMS"), or the Internet, using small, handheld mobile devices that typically have been used for telephonic communications. "Mobile operator" refers to a company that provides services to mobile subscribers; "mobile vendor" refers to a company that sells goods and services through mobile platforms, either directly, or through intermediaries including website operators (such as Yahoo! and eBay) and mobile aggregators (*i.e.* entities that assist mobile vendors by, for example, processing and forwarding multiple third-party vendor charges to mobile operators for billing to mobile subscribers); "mobile subscriber" refers to the individual who pays for a mobile phone subscription.

With the convergence of operating platforms, mobile commerce is now expanding into Internet-based e-commerce. This is making it increasingly difficult to distinguish mobile commerce from other forms of e-commerce. While mobile commerce does not as such require Internet access, ever more m-commerce transactions occur by means of communications system protocols (such as Web (HTML, TCP/IP), Wireless Application Protocol ("WAP") and i-mode) and phones connected to wireless communications networks (*e.g.* "3G"). In addition, an increasing number of personal data devices or smart phones are now able to support wireless telephonic communications.

Mobile commerce is currently growing at a rapid pace in many OECD countries. In these countries, more and more individuals have advanced mobile phones and other such devices that allow them to benefit from a broad range of mobile services that are different from what is currently possible from fixed computers. Between 1997 and 2005, the number of mobile subscribers in the OECD grew at an average compound growth rate of 24% per year (OECD, 2007b, p. 98).

Currently, mobile phone subscribers can use their devices:

- To purchase and download content, such as movies, music, ring-tones, or games.
- To play online games and gamble online.
- To access information available on a mobile screen, such as weather forecasts or the news, mobile TV and program-related information broadcast alongside TV channels.

- To obtain information tailored to data about their location through location technology.
- To access online banking and financial services, and make transactions.
- To make payments for mobile activities, either charged on credit cards or on mobile phone bills.
- As payment devices ("e-wallet") to purchase goods or services; and
- To vote in interactive TV programmes.

The development of the third generation of mobile services ("3G"), which provides high-speed Internet access on mobile phones, complete with audio and higher quality graphics, has expanded consumers' interest in the devices and opened up the potential of new commercial applications.

Another development concerns the increasing access and use of mobile phones by children. Ensuring that children benefit from mobile devices' opportunities while receiving effective protection against aggressive, inappropriate and abusive mobile marketing practices and offers represents a key challenge for all stakeholders.

Emerging mobile commerce challenges for consumers

The Committee on Consumer Policy (CCP) has been following developments in mobile commerce for a number of years. In 2007, the Committee issued a report (OECD, 2007a) providing an overview of m-commerce and identifying some of the key challenges it would pose to consumers. The report notes that mobile devices have unique characteristics that attract consumers' interest (they are easy to use and offer consumers access to service whenever they want from areas where mobile service is available), but that they also present inherent technical constraints such as small screen size, limited storage and memory capacity, battery life, and low processing power.

This document aims at providing practical measures that stakeholders could take to address a number of key issues that have emerged in countries where the market is well advanced. Other issues may well emerge over time. This document is therefore not designed to provide a comprehensive set of policy principles and actions, but rather offers some principles to guide an evolving exploration and analysis of current and future challenges posed by m-commerce. These challenges are presented below in the form of hypothetical examples.

The Committee decided to focus on three issues:

- The problems that could occur as a result of limited information disclosure possibilities on mobile devices (due to the small screens and other technical limitations).
- The increased risks of commercial exploitation of minors; and
- The heightened vulnerability of mobile devices to unauthorised use, data security breaches and privacy risks.

The Committee decided to examine these issues in light of the 1999 *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* ("the *E-commerce Guidelines*") (OECD, 1999). While most delegations considered that the

principles contained in the *E-commerce Guidelines* apply to m-commerce, they recognised that it would be beneficial to elaborate on how these principles could be effectively applied by mobile operators, website operators, mobile aggregators and mobile vendors of financial and other commercial services, as well as mobile subscribers, to address the issues mentioned above. In doing so, the Committee would also incorporate best practices from other relevant OECD instruments pertaining to consumer protection, security, privacy and spam (as listed in Appendix 2).

II. Limited information disclosure

The *E-commerce Guidelines* indicate that consumers should be provided with information, prior to contracting, to enable them to make informed decisions in their electronic transactions. Such information, which should be accurate and easily accessible at all times, is as follows (Box 1):

- Information on the business and on available dispute resolution mechanisms.
- Characteristics of the goods or services on offer; and
- Details about the transaction itself, including the terms, conditions and methods of payment, and costs.

Box 1. Key disclosure provisions in the E-commerce Guidelines

Part II of the E-commerce Guidelines set forth the following general principles:

- Section II ("Fair Business, Advertising and Marketing Practices") sets forth several general principles stating that businesses should not engage in practices that are likely to be deceptive, misleading, fraudulent or unfair; that businesses marketing to consumers should not engage in practices that are likely to cause unreasonable risk of harm to consumers; and that businesses should present information about themselves and the goods or services they provide in a clear, conspicuous, accurate, and easily accessible manner.
- Section III, C ("Online Disclosures - information about the transaction") states that the business should provide sufficient information about the terms, conditions, and costs associated with a transaction to enable the consumer to make an informed decision about whether to enter into the transaction. The information must be clear, accurate, and easily accessible and include "an itemisation of total costs collected and/or imposed by the business."
- Section IV ("Confirmation process") indicates that there should be a way for consumers to review the purchase details and make an express, informed and deliberate consent to complete the transaction. It also states that consumers should be able to retain a complete and accurate record of the transaction. They should finally be able to cancel the transaction process before concluding it.
- Section VI ("Dispute Resolution and Redress") encourages businesses to provide consumers with fair, effective, transparent and internal mechanisms to address complaints. In this regard, the 2007 OECD Recommendation on Consumer Dispute Resolution and Redress calls on the private sector to establish "[e]ffective processes for internal complaints handling, which provide consumers with the opportunity to resolve their complaints directly with the business concerned in a fair, effective, and timely manner without imposing a fee or charge for accessing or using these processes."

Providing such comprehensive information to consumers is complicated in the case of m-commerce due to mobile devices' inherent technical constraints such as small screen size and, in many devices, limited memory or storage capacity. Mobile phone offers for services or goods have typically been made in the form of SMS or mobile e-mail. In addition, they may also appear through Internet websites accessed on mobile devices. With the increased linkage of mobile devices to the Internet, even if information requirements can be technically met, they may not be sufficiently accessible to mobile phone subscribers for technical reasons.

Access to information about businesses, goods and services, and the transaction process

Offer for TV

An e-commerce retailer sent an offer for a TV to one of its customers on his mobile phone. The offer indicated that full information about the company, the TV and the terms and conditions of the sale were available on the company's website, and provided the URL. The customer ordered the item without consulting the webpage. When he received the bill, he was surprised at the high shipping and handling charges. He complained to the company, but was informed that the full details on costs were provided on the website.

In the above case, the mobile vendor seems to comply with the information requirements contained in Section III, Part II of the *E-commerce Guidelines*. However, there may be questions as to whether the information, which is only available on the Internet, would be sufficiently accessible by mobile phone subscribers. Some consumers may not have Internet access on either their mobile phones or computers. In response, governments could, acting under other provisions of the *E-commerce Guidelines*, such as Part III ("Implementation"), encourage mobile vendors to:

- Provide basic pre-contractual information by SMS, recognising that this is only a partial solution due to current limitations communications providers have made on the length of such messages and the inability to print out such information.
- Mail complete information in written form to the mobile phone subscriber expressing interest in the commercial offer.
- Provide a phone number that consumers could call to get more detailed information about their purchases.
- In addition, governments could seek to address these issues by:
- Promoting self-regulatory schemes and best practices, and encouraging private sector leadership in the development of technology to ensure that consumers can easily access the full information they need to determine whether to make a transaction.

In the future, technology aimed at providing wireless data over long distances may be helpful to the extent it facilitates transfer of data between mobile devices and computers.

Confirmation process

Unwanted subscription

A consumer using a mobile phone reached a website offering a one month free online access to a business magazine. He provided his details through SMS to accept the offer. He did not however notice the contract terms that were at the bottom of the page. They stated that after one month he would have to pay for the service; viewing the terms would have required extensive scrolling. The consumer was puzzled two months later when he received his mobile phone bill by SMS, which included a charge for the above service; he did not recall indicating that he wanted to subscribe to it at the end of the trial period.

In the above example, the consumer accessed a site, but did not confirm his intent to subscribe to that service at the end of the trial period. The service provider nonetheless claimed that the consumer had ordered the service.

The above scenario suggests that mobile phone subscribers should be given the opportunity to receive clear and full information about the proposed transaction prior to the conclusion of the contract so that they can confirm the goods or services ordered, correct any errors and to retain or print out adequate records of the proposed transaction made over mobile devices, including contract terms (*E-commerce Guidelines*, Part II, Section II and IV). If a mobile subscriber does not receive such prior information, it might be beneficial to:

- Provide mobile subscribers with an opportunity, in mobile transactions, to withdraw from the transaction process until such time as they have been provided with the possibility to review the full contract and express an informed and deliberate consent to the purchase.

In addition, mobile phone subscribers should be protected against unfair or unscrupulous mobile vendors who may, through information they obtain about the identities of persons visiting their site, exploit or harass them. To protect mobile phone subscribers from such risks, rules restricting the information (other than directory information such as name and phone number) that mobile operators can disclose without the customer's permission, to outside parties including to joint venture partners or independent contractors for marketing purposes, could be put in place in jurisdictions where existing protection is not adequate. Other mechanisms, such as rules mandating conspicuous disclosure of a mobile operator's data collection practices, could also be considered.

Stock purchase

A consumer signed on to his bank to place an order to sell stock over a mobile phone. He validated the details of the order, thinking he had confirmed the transaction. He did not realise that he had to scroll to the bottom of the validation page for confirmation information. The process for confirming the order was not clearly indicated; as a result, the transaction was not executed.

In the above example, the financial service provider had informed the consumer about the need to carry out the transaction, but in doing so, had failed to give the opportunity to confirm it. Care needs to be taken to ensure that the procedures for carrying out transactions on mobile handsets take the limitations of screen size and

storage capacity into account. Once basic information on an order has been supplied, it would be beneficial for consumers to:

- Receive confirmation of a transaction via an SMS message or e-mail.
- Provide a way for consumers to easily check on the status of their order, on their mobile handset as well as on the Internet.

Dispute resolution and redress

Section VI, Part II of the E-commerce Guidelines ("Dispute Resolution and Redress") encourages businesses to have fair, effective, transparent and internal mechanisms to address complaints. This principle is developed further in the 2007 OECD Recommendation on Consumer Dispute Resolution and Redress, which calls upon private sector participants to establish "[e]ffective processes for internal complaints handling, which provide consumers with the opportunity to resolve their complaints directly with the business concerned in a fair, effective, and timely manner without imposing a fee or charge for accessing or using these processes."

Complex chains of contracts

Interactive TV

A television talent show invited viewers to vote for their favourite contestants by sending short codes through their mobile handsets. The price of the call was disclosed only at the bottom of the screen in fine print that appeared for 10 seconds. Moreover, the print was impossible to read from the distance that viewers would normally sit from their television screens. There was no confirmation process sent on their mobile phones – after voting, viewers simply saw a message thanking them for their votes. Mobile subscribers did not realize that they had been billed for premium rate (above the cost of standard transmission) messaging services until the charges appeared on their mobile service bills. When they disputed the charges with their mobile service operators, they were informed that they had to pay the bill and take the problem up themselves with the television programme.

Mobile handset transport ticket

A consumer ordered a transport ticket from the national railway company via his mobile handset, allowing him to use his Near Field Communication enabled handset as his ticket on local buses, trains, and trams. While he was on a tram, he was stopped by a controller, who tried unsuccessfully to validate the m-ticket. As a result, the controller required him to pay for the ticket immediately and levied an additional fine because the consumer was unable to prove that he had purchased the ticket. Back home, the consumer asked his mobile operator for assistance with reimbursement for the second ticket and the fine.

The mobile operator informed him that it was not responsible in this matter and that the consumer should send his request to the railway company.

The first hypothetical case shows the interaction between two media – traditional television and commerce carried out through mobile devices. It highlights the trend towards using premium text messaging as a business model in m-commerce. The hypothetical case also raises a number of issues for mobile subscribers including: *i*) the inability of consumers to know when they are accessing premium messaging services on the mobile handsets, *ii*) the lack of a confirmation

process, and *iii*) the mobile operator's lack of an effective dispute resolution and redress system for the billing dispute.

With respect to dispute resolution, both examples illustrate a case where there is a lack of clarity as to which entity is directly responsible for handling consumers' claims. Typically, charges for mobile commerce transactions are billed to mobile subscribers by the consumer's mobile operator on behalf of the vendor of the goods or services through mobile platforms. In some cases, relationships in the delivery of m-commerce services are even more complex, notably when payment for the service at offer is debited from the consumer's bank account or credit card, as shown in the second example above.

In a few OECD countries, partnerships have been established or are being established between transport companies and mobile operators to provide consumers with the ability to use their mobile handset as a transport ticket. In these countries, consumers are charged by several methods: on their mobile phone bills, their credit cards or via cash transactions. In these multi-dimensional transactions, it should be clear to the consumer which entity has responsibility for handling consumer disputes and providing redress.

The two examples above suggest that it might be beneficial to encourage mobile operators and vendors to:

- Establish fair, effective and transparent internal mechanisms to address and respond to consumer complaints.
- Clearly indicate to consumers rules on responsibility for handling claims in complex contracts. Best practices could, in this regard, provide guidance on who, between the mobile operator, transport company or both, is accountable to consumers in light of the specific circumstances and characteristics of a case.

Moreover, m-commerce participants should consider implementing dispute resolution and redress mechanisms such as customer satisfaction codes, chargeback mechanisms, and alternative dispute resolution services, as recommended in the *2007 OECD Consumer Dispute Resolution and Redress Recommendation* ("the *Consumer Dispute Resolution and Redress Recommendation,"* Annex, Section II, A.7).

It would be beneficial for mobile operators, mobile vendors, website operators, mobile aggregators and governments to work together to establish fair, effective and transparent self-regulatory mechanisms, policies, and procedures to address consumer complaints and resolve consumer disputes arising from complex m-commerce transactions.

Cross-border disputes

Luxurious watch

A consumer received an SMS containing a link to a website, which advertised a luxurious watch at a low price. The consumer felt confident that the offer was genuine because it came from a mobile site from which he had already bought similar products and which contained information in his native language. He therefore placed an order to buy the watch. When the watch was not delivered, the consumer complained to the customer service department of the company, and found out that the business that he purchased the item from was in fact operated by another company which was not based in his country. When he complained to government authorities, he was told that they could do nothing since the business was located outside the country.

Part II, Section III, A *i*) and *iii*) of the *E-Commerce Guidelines* requires businesses to provide consumers with accurate, clear and easily accessible information about themselves (including their geographic locations) and ways to resolve disputes. Such information and redress mechanisms are necessary to help strengthen consumer confidence in cross-border transactions, as also provided for in the *Consumer Dispute Resolution and Redress Recommendation* which calls on member countries to enhance the effectiveness of consumer remedies in cross-border disputes (Annex, Section III).

Stakeholders are encouraged to establish effective dispute resolution mechanisms to address consumer complaints in cross-border m-commerce transactions.

Access to m-commerce for disadvantaged consumers

As recommended in the *Consumer Dispute Resolution and Redress Recommendation* (Annex, Section II, A. 6), the special needs of disadvantaged consumers should be addressed as m-commerce develops. For example, it may be particularly problematic for people with low vision to review disclosure/disclaimer statements on small mobile screens.

III. Protection of minors

In most OECD member countries, minors (*i.e*. generally persons under the age of 18) do not have the legal capacity to enter into commercial contracts – including, for example, contracts for voice calls or commercial transactions over their mobile devices. This does not, however, necessarily prevent them from engaging in commercial transactions using a device that is part of a contract entered into by their parents or another adult. In some countries, older minors may, however, be allowed to conclude such contracts, provided that they obtain prior parental consent. This parental control over minors' commercial activities is currently being challenged in the mobile commerce marketplace due to the sharp increase in the number of minors who possess their own devices (OECD 2006, p. 5-6). One way of discouraging minors from falsely entering into contracts would be to:

- Encourage mobile operators to put age verification systems in place.

To date, however, age verification technologies have failed to develop on a widespread basis. This is a challenging problem. Mobile operators can seek age information in a manner that discourages age falsification, *e.g*. by requiring children to enter their birthdates, rather than their actual ages. However, in the absence of age verification technologies, it is not difficult for children to evade a site's age screening mechanisms by submitting false age information, thereby gaining entrance to inappropriate sites and/or engaging in transactions without parental authorisation. This highlights the need for supplementary technology that can provide additional measures of security for children as, more and more, they engage in online activities from wireless handsets.

While parents usually aim to provide their children with mobile phones to improve communication and enhance safety, children's use of mobile phones goes much further (OECD, 2006, p. 8). They are increasingly attracted by services to which fees may be attached (such as ringtone downloads, videos, chatting, and games). As a result, they are engaging in commercial transactions, and may be exposed to risks such as *i*) access to harmful or adult content and *ii*) unexpectedly costly transactions which could result from aggressive marketing.

Part II, Section II of the *E-commerce Guidelines* provides that "Businesses should take special care in advertising or marketing that is targeted to children, …, who may not have the capacity to fully understand the information with which they are presented." This principle should guide mobile service providers, mobile operators, and others offering m-commerce services in communications and transactions with children.

Access to harmful or adult content

For adults only

A 15-year old received a text message inviting him to preview a new Internet site for free. He responded to the message and acquired the site address in return. He accessed the site, discovering that it contained sexually explicit material. He reported the offer to his mother, who contacted the mobile operator immediately, to express her outrage that her child had received the solicitation. The mobile operator explained that it did its best to filter such traffic, but some inappropriate content slipped through. When the child responded to the SMS, his contact information (i.e. phone number) was put on a list of potential customers. He subsequently received a stream of provocative messages, forcing the distraught mother to demand a new mobile phone account for her son.

Free photo site

A 15 year-old found out about a website offering adult-oriented photos for free from his friends. He went to the site using his mobile phone, knowing his parents would not be able to monitor his web activity closely. The website contained a warning that users should be over the age of 18. He responded that he was, and was granted instant access.

Businesses should consider developing more effective tools to prevent minors from accessing adult content sites from their mobile platforms. As stated in the *E-commerce Guidelines*, member countries "should… encourage continued private sector leadership in the development of technology as a tool to protect… consumers" (Part III, *iii*), "Implementation").

Much has been done to develop software that does just that with respect to screening certain content from consumers who use their computers to access the Internet. To address this issue in the m-commerce environment, voluntary codes of conduct or guidelines have been developed by mobile operators in some countries to put in place options for restricting children's access to adult content (Appendix 1). Under these frameworks, mobile operators have supported a number of ways to respond to issues involving minors, including:

- The development of awareness-raising campaigns for parents and children.
- Warning in all audio and visual advertising that interested parties must be 18 or older or have a parent's permission to participate.
- The classification of commercial content (restricted adult content versus generally accessible content); and
- The development of more effective age verification procedures.
- Additional measures that could be explored to protect minors include:
- Adapting existing member country laws and rules protecting children on line to the mobile environment.
- Encouraging mobile operators to inform parents of the filtering options available to them to help prevent children's access to adult content.
- Encouraging mobile vendors selling adult content services i) to work with the relevant authorities at domestic level to ensure effective protection of minors and ii) to put in place appropriate safeguards to prevent children's access to these services.
- Establishing procedures under which, for example, a notice could be sent to parents if their children access adult content sites; and
- Filtering services that could be activated by parents on the device to block Internet access to inappropriate content.

Marketing targeting children

Ring tones and related items

A 13-year old was intrigued by various messages she received on her mobile handset from a vendor from whom she had previously bought a ringtone. The vendor encouraged her to buy all sorts of goods and services. She ended up buying a number of additional ringtones, games, and horoscopes. Her mother asked the mobile operator to intercept the ads, but it indicated that it was powerless to do so.

Unsolicited ads

A ten-year old was shopping in the mall with his mother. As they walked past stores he was intrigued by the ads that were being beamed to him on his mobile phone by the different retailers. He showed his mother, who was impressed by this new phone feature. She was unaware of the properties of the Bluetooth technology that was installed on her son's device. When they returned home, the mother became concerned that there might be downsides to the unsolicited advertising that was now possible through the Bluetooth technology.

As set out in the *E-commerce Guidelines* (Part II, Section II), children may not have the capacity to understand fully the information that they are presented. While it may be difficult to prevent abusive m-commerce marketing that targets children, there might be possibilities for limiting it by encouraging mobile operators to put in place tools that would:

- Educate parents along with their children about aggressive marketing techniques and ways to keep spending through mobile devices in check.
- Block certain advertisers, or types of advertisers, from sending solicitations to children.
- Place restrictions on Internet content access.
- Block mobile phone purchases on devices given to children who are minors; or
- Block all mobile messages other than those from sources parents identify (known as a white list).

Mobile vendors could also be encouraged to require adult authorisation for any m-commerce purchases from parties they know to be minors.

The "Unsolicited ads" example raises a different type of challenge; in this instance, ads were beamed to the child's phone using Bluetooth technology. Such advertising was not conducted through a mobile operator and was unrecorded. The example shows that parents need to be aware of the technological capabilities and features of the mobile phone device used by their children. They need to know how these features can be modified when concerns arise.

Over-consumption of services offered by mobile operators

Soft drink vending machine

A 12-year old girl was delighted when she was elected President of her sixth grade class. At the lunch break, she decided to express her appreciation by buying a round of soft drinks for her classmates. The word spread rapidly, and soon there were 300 young friends waiting to be treated. She used her mobile phone to pay for the drinks. The total charge appeared on her mobile screen. When the monthly statement arrived at her home, her father was stunned to see the EUR 400 charge.

Interactive games

A 16-year old received a mobile phone for his birthday. His mother lectured him about not running up large charges. The young man agreed, and tried to stick to his word. However, as he saw that text messages and interactive games were very cheap, he used the services extensively, not realising that the many small charges were adding up to a tidy sum. The total monthly bill topped USD 200.

As seen in the examples above, parents may not be in a position to supervise their children's activities on their mobile handsets at all times. As a result, they may not be able to prevent them from running up substantial charges on their phone bills for services or products purchased. TV games and competitions are areas in which minors seem particularly vulnerable. As illustrated earlier in the *Interactive TV*

example, information on the costs of participation in such games is not always clearly available.

Vending machines in school premises or shopping centres are another example of temptations for minors. From their mobile phone, minors can sometimes call up a phone number indicated on the vending machine, and pay for their purchase, which will then appear on their next phone bill.

Premium rate services, as discussed earlier, may also represent temptations for young consumers. These services offer information and entertainment through a variety of media including fixed phone, fax, Internet, TV and mobile devices. Children can thus easily make a call from their mobile handset to access a wide range of services ranging from competitions, chat lines, *etc.* Typically, premium rate service calls are charged at a higher rate than standard calls. Industry can help by continuing to develop and refine technological tools to limit consumption of mobile services by minors. Such tools would be consistent with the *E-commerce Guidelines* (Part II, Section III, C. *v*) which call on businesses to provide consumers with information on the restrictions, limitations or conditions of purchase, such as parental/guardian approval requirements, geographic or time restrictions.

The approach used by credit card companies may be relevant in this regard. Once a card has been issued to an individual, the companies often allow, with the individual's consent, additional cards to be issued to other family members, under the credit limit of the principal subscriber. Credit lines can be limited and bills are sent to the principal for payment. Moreover, in some countries, minors cannot hold a credit card unless parents provide special agreement to the contract.

A few countries have gone much further (Appendix 1), placing greater responsibility on mobile operators. In one country, in the case of TV games in which participation is through SMS, mobile operators must reimburse parents for bills incurred by their children. In another country, content providers who do not set a monthly limit for the purchase of services from an access number may be considered in breach of the law.

To help prevent over-consumption by minors, stakeholders could:

- Provide parents with the ability to set a ceiling that would limit the amount of charges that children could accrue using mobile phones, by, for example, setting a limit on the number of text messages, or establishing monetary limits on downloadable purchases.
- Encourage mobile devices to be designed in a way that users could limit the types of transactions.
- Encourage mobile operators to send warnings/notices to parents when expenditures exceed an established ceiling level.

Children and location-based data[1]

Keeping track

A 12-year old mobile phone user goes on the Internet and enters her mobile phone number to sign up for a location-based service that allows her to receive information about the location of persons she has identified (social mapping). She believes this will be a fun chance to find out when her school friends are in the area so she can text message them and meet up with them. They can also receive location data and a profile about her. There is no disclosure about how such information will be safeguarded, or who can view it. There is no verification process. The location data is not blocked even when she turns off that program on the mobile device. Her parents do not know she has subscribed to such a service.

The above example illustrates challenges raised by the intersections between privacy, online activity and mobile commerce as they affect children. Other, related privacy issues, which may affect both children and adults, are discussed below in the section on "Location-based privacy and security issues". In many OECD countries, the disclosure of certain types of location-based data to third parties is illegal; however, there are still open issues regarding the extent of such protection in some countries. The lack of disclosure about tracking and the sharing of the data with third parties is magnified in many countries by the absence of a process to alert adults about these practices. Although fuller disclosure might help address the problem, it would not be sufficient.

The *E-commerce Guidelines* already set forth several general principles that might apply, including the principle that businesses marketing to consumers should not engage in practices that are likely to cause unreasonable risk of harm to consumers (Section II, Part II, 2nd paragraph); and that businesses should present information about themselves and the goods or services they provide in a clear, conspicuous, accurate, and easily accessible manner (Section II, Part II, 3rd paragraph). Here, tracking information might be considered in following the principle that the business should provide sufficient information about the terms, conditions, and costs associated with a transaction to enable the consumer to make an informed decision about whether to enter into the transaction. Such information must be clear, accurate, and easily accessible. As mentioned above, the *E-commerce Guidelines* also encourage private sector leadership in the development of technology as a tool to protect and empower consumers (Part III, *iii*)). To that end, businesses could:

- Make clear disclosures about tracking.
- Make clear disclosures about the sharing of data with third parties and how to limit it.
- Treat this as a service for which adult approval is required.
- Provide the option to turn off the specific tracking service, preferably as a default.

1 Location-based data concerns information indicating the geographical location and movement information of a mobile device.

IV. Unauthorised use of mobile handsets and security issues

The small size and functionality of mobile devices have made them attractive targets for thieves, who may be interested in *i*) re-using or re-selling the device, *ii*) carrying out commercial transactions in a fraudulent or illegal way in the name of the legitimate owner or *iii*) obtaining sensitive personal information. The risk of theft is in many ways far higher than for standard computers, which are stationary or bulkier portable computers, which are not carried around in public to the same degree.

Unauthorised use of mobile phones

Building awareness of the risks of unauthorised use of mobile phones should help to lower the number of incidents. As provided for in Section VIII, Part II, of the *E-commerce Guidelines,* stakeholders "…should work together to educate consumers about electronic commerce … to increase … consumer awareness of the consumer protection framework that applies to their online activities." Educating consumers as to what they should do in the event their mobile devices are stolen or compromised is another important aspect of preventing fraudulent use. Stakeholders should therefore work together:

- To provide information to consumers that *i*) promotes awareness; *ii*) outlines ways to protect mobile devices from loss and misuse; and *iii*) indicates what consumers should do if they discover their device has been lost or is being misused.

Buying spree

A consumer loses his mobile phone without however informing either his mobile operator or the police about it, hoping that he will find it quickly. Three days later, the police call the consumer to let him know that his phone was found. However, from the moment the phone was lost to the time that the police found it, someone used expensive mobile services from the phone, running up charges of around USD 2 000. The consumer is shocked to learn that he is liable for the full amount.

The above example underscores the importance of using the security offered by some form of encryption on the device itself as well as a PIN for some services. It also underscores the importance of timely notification when a mobile device is missing. Further possibilities to limit liability in the event of theft include:

- Enabling consumers to establish credit ceilings that may be lower than the limited liability ceilings set by handset operators.
- Providing on-demand remote services or other technical devices to enable consumers to freeze a device to prevent unauthorised use.
- Requiring that a PIN code be used for each commercial transaction carried out using the mobile device, or for accessing sensitive information on the handset.
- Educating consumers about the significance of using passwords and other technology for limiting access to such devices.

With respect to the PIN code of the SIM card, in general "0000" is assigned as an initial default PIN number.[2]

- To help deter unauthorised use, mobile operators and mobile device merchants could *i*) assign random numbers as initial PIN codes and/or *ii*) prompt consumers to change their default PIN code and set their own when they first use the device.

Busy signal

A young woman lost her mobile phone on the bus as she was returning home from work. When she discovered the theft, she immediately called her mobile operator. Several times, the line was busy. Other times, she gave up after waiting for 20 minutes for a customer representative. She was infuriated several days later when she learned that the phone had been used to purchase about EUR 1 000 of services during the time she had tried to contact the mobile operator.

Holding mobile subscribers liable for unauthorised charges made using stolen mobile devices, during a period when the subscribers were unable to notify their operator of the theft because of busy lines and the like raises questions of fairness. The inaccessibility could expose the subscribers to unreasonable risk of harm, which is inconsistent with the *E-commerce Guidelines*, and with the *Consumer Dispute Resolution and Redress Recommendation* (Part IV), which calls on the private sector to provide mechanisms for consumers to resolve their disputes at the earliest possible stages. To avoid such situations, mobile operators could be encouraged to:

- Provide sufficient means for subscribers to report their troubles easily, including, for example, through an e-mail or "online" facility for declaring lost or stolen devices.
- Set up special reporting lines for lost and stolen handsets where consumers could "key-in" information to disable the handsets.

Efforts to improve the reporting mechanisms for lost handsets have been made in a number of countries. In one country, mobile operators have teamed up and signed a charter to block cell phones reported stolen on all their networks within 48 hours. Since mobile handsets are equipped with a registered international mobile equipment identification ("IMEI") number,[3] each of the companies can place a bar on the SIM card and the IMEI via remote control to lock the handset and make it inoperable.

It should be noted that in instances where a mobile phone is used as a payment device, liability often differs from that related to the use of credit cards. In some OECD countries, consumers are, in many instances, not liable for amounts debited from a stolen credit card. When mobile phones are used as payments devices, mobile subscribers are not guaranteed the same level of protection. Mobile operators in most member countries do not cover any loss caused by the unauthorised use of SIM cards or IC chips. However, a few countries amended their legislation so as to limit the liability arising from all types of unauthorised use of communication services. To address the problem, governments and industry may want to:

2 This would not apply to the Code Division Multiple Access (CDMA) network technology which is used for mobile phones in some OECD countries.

3 Mobile handsets using the CDMA network technology are equipped with an Electronic Serial Number (ESN), which, like IMEI, is used to identify a unique mobile device.

- Explore whether there could be ways to enhance liability protection for those using mobile phones; as the E-commerce Guidelines and the Consumer Dispute Resolution and Redress Recommendation state, limitation of consumer liability and chargeback mechanisms offer powerful tools that could help protect consumers.

Foreign vacation

A woman who was spending her summer vacation in a foreign country had her mobile phone stolen from her while she was shopping in an open market. She regretted the loss but was not concerned about it being misused because the mobile operator had told her that her phone would not work in foreign countries as it was not compatible with the telecommunications network. She therefore did not report the loss, until she returned home. The mobile operator informed her of the bad news. Some USD 20 000 had been charged to her account. While it was true that her phone would not work abroad, the mobile operator had failed to tell her that the IC chip (or SIM card) could be removed from her phone and used in a different device. The company admitted that this was not clear in the information packet that they provided to her, but insisted that she pay. She took them to court where she won her case.

In the above example, the mobile operator should have provided its customer with complete information on the operation of her IC chip in foreign countries. As prescribed in Section V, Part II of the *E-commerce Guidelines*, consumers should be provided with secure payment mechanisms and information on the level of security afforded by the mechanisms. This principle is particularly important as ever more consumers use their mobile handset abroad. Efforts should therefore be made to:

- Ensure that mobile subscribers receive clear and complete information on how their mobile devices can, or cannot, be operated in foreign countries at the time they purchase their devices; and
- Warn mobile subscribers, when they purchase their mobile phone, that the IC chip of the device may be used by an unauthorised person even if the device itself may not be used abroad.

Bad loan

An office mate used his colleague's mobile device and phone number to transact a loan without authorisation. To conclude the loan, the office mate sent a message indicating the subscriber's name. The loan company did not check further the identity of the sender.

Allowing parties to use their mobile handsets to make purchases in the name of someone deviates from Section V of the *E-commerce Guidelines* on two key points: *i*) security of payments and *ii*) fair business, advertising and marketing practices (since the practice raises unreasonable risk of harm to consumers). To prevent such practice, it might be beneficial for business to put in place security procedures and tools to help identify a party in a contract concluded over a mobile device. This could be addressed, to some extent, by:

- Limiting a purchase order to the party who holds the account on the handset from which such an order is placed.
- Verifying a subscribers' identity by using information such as an SMS, a mobile e-mail address, or a PIN code.

Mobile security

Mobile banking breach

A mobile phone subscriber received an advertisement for free mobile banking services claiming that consumers could access the application anywhere and at any time with just one click. The advertisement stated that consumers could view account balances, transfer funds between accounts, and receive and pay bills, just as they do now using their home computer. It claimed that to help ensure privacy and security, all information on the mobile banking application was password-protected and encrypted and further claimed that it would protect the consumer against any unauthorised transaction. The ad contained a link to the application form, which was sent via text message. The mobile subscriber completed the application, signed up for the service, and began using it.

The next month, the mobile subscriber received a bill from her banking service provider that contained significant charges for the application and for accessing her banking data by handset. The bank's advertisements did not disclose these charges. The following month, the consumer learned that an unauthorised debit has occurred on the bank account. She attempted to have the mobile operator delete the charge but it referred her to the bank, explaining that after investigation, it appeared that the consumer's banking data had not been secured and had been compromised.

This hypothetical case raises issues for consumers including: *i*) the security of mobile handsets, particularly as payment devices; *ii*) disclosure of the costs of data access charges; and *iii*) access to appropriate dispute resolution and redress mechanisms. This section focuses on the wireless security/consumer protection issues as the other two issues are discussed above, in relation to the *Interactive TV*, *Mobile handset transport ticket* and *Luxurious watch* hypothetical examples.

Mobile devices are increasingly becoming mini-computers, which are capable of carrying out a growing range of operations, including mobile banking. The security of the wireless networks supporting the devices, both in laptops and smaller devices, is an increasingly common news topic. An intruder can break into a consumer's wireless computer or network in a way that is similar to that of most computers with Internet access – for example, through an e-mail virus. Moreover, there may be additional ways for hackers and others to obtain data from mobile devices (*e.g*. Bluetooth, Radio Frequency Identification ("RFID") chip) and infect mobile devices (*e.g*. through application downloads). Although spam and malware are currently not as prevalent on mobile devices as on computers, as the use and value of mobile transactions grows, so will interest in obtaining personal and financial data and using mobile devices for spam scams, identity theft, *etc*.

Moreover, as discussed above, the use of mobile devices to make payments is becoming more common. In some countries, mobile payments are generally conducted via SMS, or text messaging, while in other countries, mobile devices are being equipped with RFID chips that are able to transmit payment information to reading devices simply by waving their mobile device in front of a scanner in order to make a payment. This may open up new security risks.

The *E-commerce Guidelines* (Part II, Section II "Privacy") apply to this situation to the extent that they call for business-to-consumer e-commerce to be conducted in accordance with recognised privacy and security principles set out respectively in the *1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flow of*

Personal Data ("the Privacy Guidelines"), the *2002 OECD Guidelines for the Security of Information Systems and Networks*, and taking into account the *1998 OECD Ministerial Declaration on Protection of Privacy on Global Networks*. There may, however, be a need for additional measures. It might be beneficial for participants in mobile commerce to:

- Ensure that consumers are informed about the potential security and privacy challenges they may face in m-commerce and the available measures which can be used to limit the risks.
- Encourage the development of security precautions and built-in security features.
- Encourage mobile operators to implement data security policies and measures to prevent unauthorised transactions and data breaches; and
- Provide consumers with timely and effective methods of redress when their data is compromised and/or they suffer financial loss.

Location-based privacy and security issues

Unauthorised tracking

A mobile operator uses a Global Positioning System ("GPS") or triangulation (from signals generated from the device) to locate mobile users. The company sells the location and subscriber information to marketing companies for use in sending tailored advertisements or notices to the mobile subscriber. The mobile subscriber has not understood nor has she authorised transfer of such personal information. She might be charged for the notices (e.g. text messages about nearby sales or Internet time for pop-up messages). She is disturbed by the tracking and concerned that the information could be picked up (stolen or bought) by criminals.

The above example illustrates challenges raised by location-based information tracking. At issue is the lack of a process to safeguard information and, as in the hypothetical example discussed earlier in relation to the protection of children (*Keeping track*), the lack of a mechanism to disable tracking for non-emergency purposes.

The need for protections to safeguard location-based information might be addressed by the principle in Section VII, Part II of the *E-commerce Guidelines* that business-to-consumer electronic commerce should be conducted in accordance with recognised privacy principles set out in the *1980 Privacy Guidelines* (Part II, 7-10) and taking into account the *1998 OECD Ministerial Declaration on Protection of Privacy on Global Networks*.

It would be beneficial for businesses to:

- Provide consumers with clear disclosures about any location information that is being collected and the intended use of such information.
- Provide consumers with the opportunity to limit the sharing of data with third parties (except in emergency situations), and to revise their decisions about whom such data can be shared with.

In addition, companies that collect location data should take appropriate steps to safeguard such information, particularly when the data are sensitive or can be traced back to a particular individual.

Appendix 1: Protecting minors: laws and self-regulatory schemes in some OECD countries

Access to adult content

Actions have been taken in a number of countries to address the challenges that mobile phones present. In Australia, Denmark, Germany, Japan, Korea, Norway, the United Kingdom and the United States, for example, mobile operators have developed voluntary codes of conduct to restrict access to adult content. In the United States, some mobile operators have adopted voluntary content classifications and Internet access controls to limit adult content access and enable parents to control it (see www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36). Under these guidelines, participating carriers currently block all adult-oriented content websites and would restrict access to such content through a portal only accessible to consumers at least 18 years of age or when authorised by a parent or guardian. Moreover, the Children's Internet Protection Act ("CIPA") requires schools and libraries participating in the E-rate program – a program that makes certain technology more affordable for eligible schools and libraries – to certify that they have an Internet safety policy including technology protection measures to block or filter Internet access to material that is obscene, contains child pornography, or is harmful to minors.

In addition, the Mobile Marketing Association ("MMA"), an international group that has guidelines in both Europe and the United States, has recently revised its US best practices guidelines for marketing to youth under the age of 13 (see http://www.mmaglobal.com/bestpractices.pdf). The guidelines, for example, provide that for audio and visual disclosures, participants must be at least 18 or have parental permission. Likewise, in February 2007, leading European mobile operators agreed on a European Framework on Safer Mobile Use by Younger Teenagers and Children (see http://ec.europa.eu/information_society). Under this framework, mobile operators support the development of awareness raising campaigns for parents and children; classification of commercial content (restricted adult content versus generally accessible content); and the development of age verification procedures.

Protecting children's personal data

Countries could explore adapting existing laws and rules protecting children on line to the mobile environment. For example, in the United States, federal law restricts the collection, use, or disclosure of personally identifiable information from and about children under the age of 13 in online services. This includes notification about privacy policies; verification of parental consent for collecting personal

information from children (with limited exceptions); parental review and deletion of personal information from their children; and requirements for procedures to protect the security of the data.

Over-consumption of services offered through mobile phones

Some countries have gone much further, placing greater responsibility on mobile operators. In Finland, the Consumer Complaints Board has established the responsibility of service providers in a case involving TV games played with text messages. The mobile operator was found to have received unfounded gains. The fact that a parent had allowed his/her child to use the parent's telephone did not in itself permit the child to legally enter into a commercial transaction such as the TV game in question. Under the decision, the consumer was eligible for a refund.

Marketing targeting children

The *E-commerce Guidelines* recommend that businesses should take special care in advertising or marketing that is targeted at children as they may not have the capacity to fully understand the information presented to them. Similarly, the MMA guidelines *(para*. 4.0), state that offering "programs that engage children in the promotion/consumption of digital content of any type imposes important ethical considerations, responsibility, and sensitivity that all industry participants are expected to uphold." While some countries have laws or regulations limiting such marketing, few have provisions pertaining specifically to mobile commerce. One exception is the United Kingdom, where junk food advertisement targeting children through mobile phones has been banned.

The US version of the MMA guidelines for short and multimedia wireless messages directed to children under 13 (see para. 4.0) call for all wireless industry participants to disclose that the service is a premium charge (when applicable) in all advertising in audio and visual; the actual cost of the charge and; if applicable, the fact that the standard messaging fees also apply. The guidelines also state that the word "free" may not be used unless there are no fees or charges associated with the service.

In Finland, the Guardianship Services Act provides that minors may only perform transactions which are usual for their age and have little significance. Under the Finnish Communications *Market Act*, the Finnish Communications Regulatory Authority defines *barring categories for telecommunications*. Subscribers, for example parents, can themselves determine the types of additional-cost services they want to block calling or texting to. Barring a certain category of services blocks all services which belong to the category in question. The Consumer Ombudsman has also negotiated some improvements in relation to the status of minors as subscribers of mobile services and has co-operated with businesses in that regard. Attention has been drawn to system maintainers' own responsibility for the system they use and compliance with already existing legislation. The Consumer Ombudsman has also drawn mobile operators' attention to their responsibility as the billing entity, including handling claims and compensation, as appropriate.

Unauthorised use of mobile phones

In Finland, the issue of the identification of the contracting party has been examined. The Ministry of Justice has, for example, set up a working group to draft a Government bill amending legislation on SMS instant loans. Consumer identification is currently only based on information about mobile subscriptions and social security numbers. The working group will consider whether there should be a statutory obligation for credit providers to identify customers in a more reliable way.

Privacy considerations

The Finnish *Act on the Protection of Privacy in Electronic Communications* requires that permission must be obtained from consumers before electronic direct marketing can be sent to them. The Data Protection Ombudsman and the Consumer Agency/Consumer Ombudsman have for example developed guidelines in relation to the so-called "tell a friend" marketing practice, which requires permission in advance from the recipient ("tell a friend" marketing refers to consumers forwarding product tips, introductory offers, contest invitations and other marketing messages to people they know by e-mail or text message).

The Finnish Act on the Protection of Privacy in Electronic Communications covers also confidentiality of identification and location data. This includes limits to the processing of identification data, such as processing for marketing purposes, and limits to the processing and disclosure of location data. It also covers the requirement of service-specific consent of the party to be located. In the case of minors under the age of 15, the guardian is responsible for deciding on the processing of location data.

In the United States, a carrier's ability to transmit users' location information to third parties is limited by statutory rules regarding the use of Customer Proprietary Network Information ("CPNI"*).* Specifically, Section 222 of the US Federal Communications Act prohibits the disclosure or use of wireless location information, obtained by a carrier by virtue of its provision of telecommunications services, without the express prior authorisation of the customer, except in specified emergency situations to respond to a wireless user's emergency call or in the transmission of automatic crash data. Further, the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN SPAM") Act prohibits mobile service commercial messages from being sent directly to wireless devices through the Internet without a subscriber's express prior authorisation. Additionally, the United States' Telephone Consumer Protection Act ("TCPA") prohibits any call using an automatic telephone dialing system or an artificial or prerecorded message to any wireless telephone number, including both voice calls and text messaging calls to wireless phone numbers.

Appendix 2: OECD instruments addressing mobile commerce issues

Consumer protection instruments

1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce.

2003 OECD Guidelines for the Consumer Protection against Fraudulent and Deceptive Commercial Practices Across Borders (OECD, 2003), which establish a framework to combat all sorts of offline and online fraudulent activities at both domestic and international levels.

2007 OECD Recommendation on Consumer Dispute Resolution and Redress (OECD, 2007c), which aims at providing consumers with effective mechanisms to settle their claims and obtain redress, whether at domestic or cross-border levels.

2008 OECD Policy Guidance on Online Identity Theft.

Security, privacy, and anti-spam instruments

2002 OECD Guidelines for the Security of Information Systems and Networks (OECD, 2002), which set out principles to ensure consistent domestic approaches in addressing security risks in a globally interconnected society.

OECD (2007d), *Recommendation and Guidance on Electronic Authentication*, OECD, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.

1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980), which contain principles on the collection and processing of personal information.

2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (OECD, 2007e), which calls on member country authorities to co-operate with foreign authorities and assist each other in the enforcement of privacy laws.

2006 OECD Anti-Spam Toolkit of Recommended Policies and Measures, which aims at facilitating international co-operation in the fight against spam and provides a set of recommendations to put in place complementary policies in the enforcement of anti-spam initiatives among OECD member countries.

BIBLIOGRAPHY

EC (European Commission) (2006), *Special Eurobarometer Safer Internet*, May 2006, http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf.

EC (2007), *12th EU Implementation report on European Electronic Communications Regulation and Markets*, COM(2007)155, 29 March 2007, http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/12threport/com_2007_155_en.pdf.

ITU (International Telecommunications Union) (2004), *Mobile phones and youth, a look at the US student market*, February 2004, www.itu.int/osg/spu/ni/futuremobile/Youth.pdf.

OECD (Organisation for Economic Co-operation and Development) (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* OECD, Paris, www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

OECD (1999), *Guidelines for Consumer Protection in the context of Electronic Commerce*, OECD, Paris, www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html.

OECD (2002), *Guidelines for the Security of Information Systems and Networks*, OECD, Paris.

OECD (2003), *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/sti/crossborderfraud.

OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, OECD, Paris, www.oecd-antispam.org/.

OECD (2007a), *Mobile Commerce*, DSTI/CP(2006)7/FINAL, www.oecd.org/sti/consumer-policy.

OECD (2007b), *OECD Communications Outlook 2007*, OECD, Paris, http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF.

OECD (2007c), *Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, www.oecd.org/dataoecd/43/50/38960101.pdf.

OECD (2007d), *Recommendation and Guidance on Electronic Authentication*, OECD, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.

OECD (2007e), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, www.oecd.org/dataoecd/43/28/38770483.pdf.