Industry Code of Practice

For the use of mobile phone technology to provide passive location services in the UK

24 September 2004

TABLE OF CONTENTS

1. Introduction

It is expected that many location services using mobile phone technology will be launched into the market and that the benefits to consumers will be substantial.

The purpose of this Code of Practice is to set principles of good practice for the provision of such services. They have been developed by a working group comprising of nine leading location service providers ("LSP") in the UK and the five mobile network operators. A list of participants can be found in Annex H.

The working group will subject the Code of Practice to regular review, so that it remains relevant to the needs of customers and industry and compliant with applicable law. **All** LSPs using location data supplied by mobile network operators in the UK should, at minimum, observe this Code of Practice.

Location services may be either 'active' or 'passive'. 'Active' location services are those that are initiated directly by the mobile phone user. An example of such a service is *"Where's my nearest chemist/cash machine/cinema etc.?"*

A response from the LSP would typically supply this information to the customer in the form of an address, a map or directions, based on the customer's location. The working group does not believe that there are significant safety issues associated with such 'active' location services.

This Code of Practice focuses on 'passive' location services, which are defined as those services where a mobile phone user, once s/he has enabled the service, consents to be located by another, when that other person initiates a location request (either from another mobile phone or from a PC). They do not relate to the day to day operation of a mobile network, where location data is used to pass incoming calls to customers or used by the emergency services to allocate 999 calls to the correct local emergency service.

Industry and the public alike do not want location services to be used to locate customers, particularly children, either without their knowledge or against their will. As with everything, risk cannot be completely eliminated and so the Code of Practice seeks to balance usability with safeguards in a proportionate and reasonable manner. For the purposes of developing the Code of Practice, services are broken down into four main types:

A. Child location services

B. Friend location services

C. Mobile games supported by location services

D. Corporate location services

Annex F includes a section *"Location services and you"* which provides information on the Code of Practice and additional safety messages which will be used for awareness raising by LSPs supporting this Code of Practice, for example on web-sites explaining the use of location services.

2. General principles

This Code of Practice is designed to provide consumer (particularly child) protection measures that supplement the legal and regulatory requirements such as privacy and data protection legislation (including Regulation 14 of the Privacy and Electronic Communications regulations 2003 – Restrictions on the processing of location data, which is laid out in Annex G).

The Code of Practice does not constitute legal advice nor does it seek to interpret privacy and data protection legislation, which applies to both active and passive location services. LSPs should seek their own advice regarding the application of the law to their service.

The Code of Practice is underpinned by some general principles:

- Location services must be consent-based and simple for consumers to understand and use with confidence
- Where practical, in the interests of simplicity, recommended industry standard text should be used for obtaining consents, sending alerts and stopping or suspending services
- Location services should not be used to undermine customer privacy and, in particular, should not be used for any form of unauthorised surveillance
- Alert messages should be sent at random to guard against consumers being located without their knowledge
- Location services should be easy to stop or temporarily suspend
- Advice on how to use location services and key safety messages should be readily at hand

Advice to consumers

LSPs must make available information on their web sites (which should also be accessible via WAP) and through other material on how their location services operate. This should include the standard text of *"Location services and you"* which has been agreed by the industry - see Annex F.

Advice to consumers must encompass at least:

- service terms and conditions;
- conformity with data protection legislation;
- how to contact the location service provider's customer service, including by telephone;
- how locatees can access information about who can locate them;
- key safety messages, including instructions on how to stop or suspend any location service offered; and
- The LSP's approach to the disclosure of location data when a locatee's handset is switched off.

- Confirmation that the service complies with the Code of Practice for the use of passive location services in the UK
- Include a copy of the Code or a link to the Code on the MBG web site
- Explain how to complain to the MBG about instances of non-conformance with the Code.
- Reference to the Privacy and Electronic Communications Regulations

3. Specific provisions

A. Code of Practice for child location services

This part of the Code of Practice lays out the procedures that should be followed by providers of passive location services which can be used for locating children (whether customers register remotely for the services via a web site, through a call centre or a retail shop). These services are typically configured in a way that allows the mobile phone or other device used by the child (the locatee) to send its location to the mobile phone or PC used by the parent/carer (the locator), either at regular intervals or at the request of the locator.

For the avoidance of doubt, where the age of both locator and locatees has **not** been verified (as per the Adult/Friend Finder service), the Child Location service process should be used, whether the intended locatees are children or not.

1. Identity Verification

It is fundamental to this Code that parents are confident that child location services are not readily open to abuse. To that end the Code targets identity verification as requiring sequential 'layers' of validation and safeguards as a proportionate response to risks.

The following procedures are based upon the reasonable endeavours of what can be achieved now – i.e based on public databases that are currently available to commercial companies – and the existing arrangements are being kept under review. At the same time the process recognises that registration for location services could utilise the Internet as well as visits to retailers, and that both electronic and other forms of payment will be possible.

The three primary aspects of the Codes relate to:

- The identity of the locator (normally parent or guardian)
- The relationship between the locator and the locatee (normally a child)
- Dealing with consent of the locatee before location information is revealed

2. Identity of the locator

Location Service Providers will seek to establish and then to verify the name, address and, if applicable, mobile telephone number of an applicant before the ability to locate another mobile telephone is activated. The following data sources will be used:

- External - reputable agencies (such as Dun & Bradstreet; Experian or Equifax) that use a broad range or data sources to carry out either identity checks or credit checks OR using a credit card clearing house that uses name and address information to validate a transaction OR the provision of two original (ie not photocopies) official documents that are less than 4 months old (such as a utility bill, bank statement, council tax bill, TV licence or driving licence) containing the name and address of the applicant.

- Internal – existing customer, equally robust, data held by the location service provider on the applicant.

As an additional precaution applicants will be encouraged to use a credit card at the point of registration as in some cases this may permit further validation.

When applicants are registered through a web site, an e-mail address must be captured. Following registration, an e-mail validation code (or web based link) must be sent to the e-mail address and the user must respond to the code in a pre-determined way confirming the e-mail address before location requests can be made on the account. (This is in addition to the PIN sent to the postal address, as per next paragraph).

Following satisfactory checks, a unique PIN confirmation will be sent to the locator's postal address in the United Kingdom. For this purpose a foreign address, PO Box numbers or other known accommodation addresses will be excluded.

Location services will not commence until PIN code has been returned. A full audit trail will be kept of those registered; the methods used to validate identity and the name/mobile telephone number of the person who the locator is approved to seek to locate.

3. Relationship between the locator and the locatee

The LSP must ask the locator to confirm the date of birth of a locatee. If a child under the age of 16 is to be located, the first locator opening an account with an LSP must be the child's parent or legal guardian.

The locator must make a declaration of his or her specific relationship to the child being located.

To facilitate family use of location services it is permissible for a parent or legal guardian to act as a master locator, register for a service and then add other handsets or devices belonging to additional locators.[1]

If the prospective locator gives the location service provider any reason to doubt the relationship claimed, then documentary evidence may be required to resolve the uncertainty.

[1] The master locator's account must be protected by a username or customer number and a secret password so that unauthorised handsets cannot be added without the master account holder giving consent.

Explanatory literature must make it clear that the master locator assumes responsibility for management of the account, including the activities of the other locators.

4. Consent of the locatee

There are some practical difficulties in establishing whether young children have the ability fully to understand the implications of consenting to their location being passed to others.

As a first safeguard, therefore, if the locatee is under 16, the parent or guardian must give consent to the child signing up to the location service. In addition, the child should also consent. If the child does not consent, his or her wishes must not be overridden and the service must not be activated. In the event that the child does not have the capacity to give consent, the consent of the parent will suffice.

The request for consent must follow the text shown at Annex B and only be accepted when identified as being sent from the l device that is to be located. Further, such a message must include a previously issued activation code (or some similarly secure technique) known only to the locatee. If consent is refused or fails to comply with the method of confirmation, then the service will not be activated even if requested by a parent.

5. Information to locatee

The next safeguards apply once registration has been completed. First, locatees can request from the location service provider, a list of all names and telephone numbers of persons authorised to track their mobile telephone via the service.

6. Random alerts to locatee

Second, the locatee must receive random SMS alerts to remind them that their mobile telephone is registered so that others can identify their location. The text and frequency of such messages is shown at Annex C. If an alert is not delivered for whatever reason, it will continue to be sent until delivered. Alerts should be sent at random intervals, not in a set pattern.

7. Marketing and promotion of child location services

a) Child Location Services should not be marketed in any way which exploits parents' concern or fear that their child may become a victim of crime.

b) Child location services should be marketed appropriately, taking account of the fact that knowing where the child's phone is does not necessarily tell you of the location of the child or that he or she is safe.

In order to guard against unwarranted claims being made in the promotion of these services, all printed and on-line marketing collateral associated with the product should include the following standard statement agreed by industry :

"Location Services are designed to locate the phone of another person. For the service to work, the phone has to be switched on and within network coverage. Location services aimed at children are intended to complement, not be a substitute for, normal parental supervision. They give information about the location of a child's phone and, in conjunction with other types of communication, such as phoning or texting, can help parents keep in touch with their children"

For advertisements in the print media **only**, it is permissible to use the following shortened version, providing that in all other instances the full version is used:

"Location services are intended to complement not substitute parental supervision. For a phone to be located, it must be switched on and in network coverage."

8. Stopping or suspending the service

Finally, a simple way to stop a location service, either temporarily or permanently or to remove one or more of the registered locators is set out at Annex E.

9. Additional note on Consent and reminders

As an alternative to the exchange of SMS for the collection of consent and the sending of reminders using text messages, LSPs may use voice calls direct to the locatee's phone – **providing that** an auditible record can be kept of the consent being collected and the reminders being given.

B. Code of Practice for Adult/friend location services

This part of the Code lays out the principles of good practice that should be followed by providers of passive location services supplied for the purpose of locating adults/ friends (whether customers register remotely for the service via a web site, through a call centre or a retail shop), where all participants (locators and locatees) have demonstrated, through age verification, that they are at least 16 years old.

For the avoidance of doubt, where the age of both locator and locatees has **not** been verified, the Child Location service process (as set out in part A) should be used, whether the intended locatees are children or not.

The objective of the Code of Practice is to lay down practical steps to combat misuse. LSPs may exceed the minimum standard of controls as they see fit.

1.1 Age Verification

Adult/Friend Location Services should only be made available to those that the LSP - or serving MNO - has verified are 16 years old or over.

LSPs must use a robust form of age verification[2]. For example LSPs could carry out a credit card transaction on the customers credit card (not a debit card, as they are available to under 16s). A list of the evidence that is accepted as proof of age during the signing up process must be kept. The list must be provided to mobile operators on request.

The attention of the prospective locator must be drawn to any relevant terms and conditions and the prospective locator must confirm their acceptance.

1. 2. Consent

LSPs must (under Privacy and Data Protection legislation) obtain from all locatees consent to being located before any location service is activated. Recommended text is laid out in Annex B.

The LSP must check that the consent is being sent from the device that is to be located. Consent should be confirmed by the return of an activation code known only to the locatee or some other mechanism, which can be demonstrated to be equally secure, to ensure that the consent is being sent from the locatee's device and not a PC or some other mobile device.

In addition customers must be provided with clear safety advice at service commencement. This should include appropriate and unambiguous advice to locatees to consent to the operation of friend location services, only where they know the prospective locator.

---

[2] **Age verification** – a process by which reasonable and practical steps are taken to verify that a customer is 18 or over. Acceptable methods of age verification include: –

a) "customer not present": a valid credit card transaction for the customer; age confirmation using 3rd party agencies (e.g. Experian or Dun & Bradstreet etc.)*;*

b) documents and/or process used for contract mobile phone customers, combined with a process by which customers can manage access controls.

As an example, the following message (or some similarly unambiguous equivalent) must be sent to the locatee as an SMS [in tandem with the request for consent]

WARNING: [SERVICE NAME] ALLOWS OTHER PEOPLE TO KNOW WHERE YOU ARE. FOR YOUR OWN SAFETY MAKE SURE THAT YOU KNOW WHO IS LOCATING YOU.

Reciprocity

Friend location services may be provided on a reciprocal basis between two individuals. Once individual A has requested and received consent to locate individual B, a reciprocal right is automatically conferred on B. The principle of reciprocity should then be maintained at all times.

If individual A withdraws consent (permanently or temporarily) to be located by individual B then by automatic default individual A may not locate individual B so that the principle of mutual location is not broken.

1.3. Random alerts to locatee

Subsequent to activation, the LSP must send periodic SMS alerts to all locatees to remind them that their mobile phone can be located by other parties. These alerts should be sent at random intervals, not in a set pattern. The suggested text and minimum standard frequency for sending the alerts is set out in Annex D

If an alert is not delivered, for whatever reason, it must be re-sent until it is delivered. Even if no location requests have been made in relation to a locatee since the previous alert was sent the alert must still be sent.

1.4. Information to locatees

Locatees should be able to receive on request from the LSP a list of all names of people authorised to track their phone via the service.

1.5. How to stop a service

There should always be a simple way to stop a location service either temporarily or permanently or to remove one or more of the registered locators. Examples of how to do this are laid out in Annex E.

1.6 Introduction services

Location Services, which are used to facilitate the introduction of customers who are not known to each, should only be made available to those that the LSP - or serving MNO - has verified are **18** years old or over.

Where an individual has given a consent to be located in advance of any request from a locator, some of whom may not have been previously known to him or her, there must be no presumption of the reciprocity of the consent.

C. Code of practice for mobile games (and similar services) supported by location services

This part of the Code lays out the principles of good practice that should be followed by providers of mobile games (and similar services) which are integrated with passive location services.

Where games include features that could lead to strangers being introduced to each other or the location of one stranger being revealed to another these features should not made available to customers under the age of 18, unless the identity and address of all players have been verified.

The objective of the Code of Practice is to lay down practical steps to prevent misuse. LSPs may exceed the minimum standard of controls as they see fit.

1. Traceability of players

Where a game includes the following features:

- games are multi-player, and include the option of strangers pitted against each other; and
- geographical location information is used as part of the game; or
- the game allows unmoderated chat between players

The LSP must verify that all customers playing the game are 18 or over. Alternatively, and providing no unmoderated chat is offered, the LSP can offer fully fledged games to those under 18, where the address and identity of all players in a game have been verified, using the documentation approved for Child Location Services.

Location information, where provided, should only be available for the duration of the game.

2. Protection of customers under 18

Where the LSP has not verified that all players in the game are either at least 18 or has not verified the name and address of all players, the games provider must adhere to the following Code of Practice:

- Players identities/MSISDN should not be given out to other players – they should use an alias
- True physical location information which would reveal the whereabouts of players should only be obtained by games providers for the purposes of the game and should not be given out to other players;
- Games are therefore based in a virtual world or location feeds are mapped in such a way that they do not disclose the identity of players, actual location or the actual distance away that one player is from another;
- No physical safe-havens or sponsored locations are permitted within the game which would facilitate players meeting up for example Treasure Hunts;
- No linked chat facilities are permitted unless they are moderated and cannot be used to make actual contact. Such moderation may include the use of templates (i.e. a set of fixed phrases) pre-defined by the LSP.

3. How to stop a service

There should always be a way to stop a mobile game supported by a location service either temporarily or permanently. When a mobile game supported by a location service is stopped or suspended location information should no longer be provided.

D. Code of Practice for corporate location services

This part of the Code of Practice lays out the principles of good practice that should be followed by providers of passive location services to corporates such as businesses, local authorities, charities and other organisations.

These services are typically configured in a way that allows a mobile device fixed in the corporate's vehicle or of an employee or of an associate (the locatees) to send its location to the mobile phone or PC of the corporate customer (the locator), either at regular intervals or at the request of the locator. This part of the Code applies where the service is sold to the corporate customer by the LSP or its agents through a face to face transaction. Where the customer signs up remotely – through the Web, a call centre or a retail outlet, Part A or B is the appropriate Code (depending on whether customers are verified to be over 16 or not).

Another use of a corporate location service is for marketing and promotion of goods to customers and potential customers. This topic is covered in more detail in section 4 below.

The objective of the Code of Practice is to lay down practical steps to prevent misuse. LSPs may exceed the minimum standard of controls as they see fit.

1. Traceability of *bona fide* corporate customers

LSPs should verify that their corporate customer is a *bone fide* organisation. They must verify the name and address of the corporate customer that has registered to locate mobile phones used within or in association with the organisation, before service commencement.

Examples of verification of a corporate customer may include the use of:

- company registration including registered address and proof that an organisation is trading such as evidence of employment liability insurance,
- banking or credit validation using reputable agency e.g. Dun & Bradstreet, Experian or Equifax, or
- verification of the identity and address of Directors or other responsible individuals.

Examples of verification of the identity and address of Directors or other responsible individuals may include the use of combinations of:

- copies of identity and address documentation such as that required for contract phone provision;
- other reputable identity documentation such as Citizencard;
- a valid credit card transaction at point of registration;
- a unique PIN confirmation sent to a locator's postal address in the UK (not including a PO Box address), where the location service does not commence until the address is confirmed and / or
- Identity Validation Check using reputable agency e.g. Dun & Bradstreet, Experian or Equifax.

LSPs must maintain a list of all corporate customers including an audit trail showing the validation method used. LSPs must be able to provide proof of identity validation including the corporate customer's name and address upon request.

2. Consent or confirmation of mobile devices within corporate control

For corporate location services, LSPs may choose to confirm individual locatee consent followed by the use of random notification mechanisms detailed within Annex D.

Where an LSP does not use this approach it must satisfy itself that all corporate customers have taken sufficient steps to obtain the necessary consents from the users of the mobile devices that are subject to the location service. LSPs must be able to provide proofs of consents upon request from a MNO.

3. The corporate customers' responsibilities

LSPs must, through their contract terms and conditions, make it clear that it is their customer's responsibility to use the service within the law, including all relevant privacy and data protection legislation.

The location service provider's contract must state clearly that its customer will be responsible for managing the processing of location data and distributing information to their employees or associates about the service and how it operates.

The location service provider's terms and conditions must lay down the consequences of misuse by its customer. These may include service suspension and, in cases of persistent mis-use, service withdrawal.

4. Location notification

In order to protect against the location service being used for unauthorised or accidental surveillance of individuals that are not employees or associates of the corporate customer, LSPs must send out or ensure that their customers send out a confirmation SMS or e-mail to a mobile device which is the subject of a business location service. Where there is no text or email enabled, notification to the locatee must be sent in writing to the locatee's address.

As an example the following text may be sent to a device once a location service is enabled:

"[CORPORATE CUSTOMER'S NAME] can locate this phone at any time. Should you have any questions please contact please call [CORPORATE CUSTOMER PHONE NUMBER] or send STOP [SERVICE NAME] to [SERVICE NUMBER]. [SERVICE WEBSITE] by [PROVIDER NAME]."

5. Promotions and competitions

Companies may want to use location services for marketing campaigns and competitions. In some cases these are clearly Active services but in others, the location look up will be done at sometime after registration and therefore is a Passive service.

Examples of 'passive' uses are given below:

i) Competition advertised on wrappers/labels/posters etc. User sends a text to enter the competition and by doing this consents that their location maybe used at some defined point in the future as part of the competition. All terms and conditions will clearly state that location may be used, will provide specific details of when location information will be used and the customer's details will only be kept for the duration of the competition.

ii) Promotion will encourage users to sign up to a specific campaign where over the period of the promotion the location may be requested several times, and they will be advised of special offers etc near where they are. They may also be encouraged to be in specific locations at certain times.

Should any such promotions or competitions facilitate more than one entrant being in the same location(s) at the same time(s), the promotion or competition should only be targeted at or be open to customers that have been verified to be 18 or over.

To avoid duplication the Industry Code of Practice refers out to section 10 of the Mobile Marketing Association's Code of Conduct (published December 2003 at www.mmaglobal.co.uk)

10. Are there any special requirements if I am using location based mobile marketing?

The collection and use of location data relating to individuals is subject to specific legal requirements, in particular those set out in the Electronic Communications Regulations.

If you are planning to collect or use such data in any way you must make sure that you comply with these requirements.

In addition, you must:

- only send location based mobile marketing (i.e. mobile marketing which is sent based on the location of the recipient at a given time) to people who have specifically agreed to receive this type of marketing; and

- each time you send a location based mobile marketing communication provide the recipient with a simple free of charge (other than the costs of transmission) means of opting out of receiving any further such location based mobile marketing communications at any time.

When asking people to opt in to receive location based mobile marketing you must make clear to them:

- that in order to send them such marketing it will be necessary to identify the location of their mobile device and so their personal location; and
- what you will be using these location details for.

ANNEX A - Glossary

Associates: An individual that is contracted to work for a corporate customer, such as an agency temp or sub-contractor.

Locatee: The person being located in a passive location service.

Locator: The person initiating a location request in a passive location service.

Location services: services that are supplied to mobile phone users, drawing on the location information derived from mobile phone networks.

Location service provider ("LSP"): A value added service provider who offers a service using location information provided by a mobile phone network or through the use of a satellite positioning system.

Mobile network operator: The five network operators in the UK are O2, Orange, T-Mobile, Vodafone and 3.

Passive location services: those services where a mobile phone user, once s/he has enabled a service, consents to be located by another, when that other person initiates a location request (either from another mobile phone or from a PC).

WAP/WML: Wireless Application Protocol and Wireless Mark up Language; the protocol used by mobile phones to browse content sites (including those on the Internet) written in WML.

ANNEX B - Obtaining consent (for child location and adult/friend location services)

All locatees must provide to the LSP a consent to be located before any location service is activated

Before giving his or her consent, a locatee must be informed of the following:

- that someone wishes to locate their mobile phone;
- name and phone number of prospective locator;
- website or customer support number where further service information including safety advice and terms and conditions are available; and
- the service name and location service provider name.

As an **example** the following text may be sent to the locatee as an SMS when a locator first requests the ability to locate them:

"[NAME] [PHONE NUMBER] wants to locate your mobile from now on. Text [SERVICE NAME] YES [NAME] +[activation code] to [SERVICE NUMBER] to agree. [SERVICE WEBSITE] by [PROVIDER NAME]."

The request for consent should refer to a web site or other materials, where detailed information can be obtained about the nature of the service, safety advice and the rights of the locatee.

If consent is refused, the service must not be activated – even if the location service has been requested by a parent.

ANNEX C - Random alerts for child location services

Subsequent to activation, the LSP must send periodic SMS alerts to all locatees to remind them that their mobile phone can be located by other parties. These alerts should be sent at random intervals, not in a set pattern.

The following minimum standard for the frequency of notifications must be maintained (alerts should not be sent between 10pm and 7am):

Period	Notification
After 3 hours but within first 24 hours of first consent being given	At least 1 SMS
Within 24-48 hours	At least one SMS
48 hours to 1 week	At least 1 SMS
1 week to 2 weeks	At least 1 SMS
2 weeks to 4 weeks	At least 1 SMS
Every subsequent month	At least 1 SMS

Even if no location requests have been made in relation to a locatee since the previous notification was sent, subsequent notifications must be sent in accordance with the above periods.

Random notifications to locatees must contain the following information:

- name and phone number of all persons who can locate their phone;
- the notification must provide the individual with sufficient information to allow them to stop the service if they wish to do so; and
- website or customer support number where further service information including terms and conditions are available;

As an example the following text may be sent to the locatee to remind them that a location service is still active:

"[NAME] [PHONE NUMBER] can locate your phone at any time. To stop this service please send STOP [SERVICE NAME] [NAME] to [SERVICE NUMBER]. [SERVICE WEBSITE] by [PROVIDER NAME]."]

If this message is not delivered, for whatever reason, it must be re-sent until it is delivered. Even if no location requests have been made in relation to a locatee since the previous alert was sent the alert must still be sent.

If the LSP receives no delivery receipt for the reminder SMS after 4 attempts or a maximum of 48 hours, the locatee must be suspended from the service. Before the locatee is reinstated on the service, a fresh consent must be obtained.

ANNEX D – Random alerts for adult/friend location services

Subsequent to activation, the LSP must send periodic SMS alerts to all locatees to remind them that their mobile phone can be located by other parties. These alerts should be sent at random intervals, not in a set pattern.

The following minimum standard for the frequency of notifications must be maintained (alerts should not be sent between 10pm and 7am):

Period	Notification
After 3 hours but within first 24 hours of first consent being given	At least 1 SMS
24 hours to 48 hours	At least 1 SMS
48 hours to 2 weeks	At least 1 SMS
2 weeks to 4 weeks	At least 1 SMS
Every subsequent month	At least 1 SMS

Even if no location requests have been made in relation to a locatee since the previous notification was sent, subsequent notifications must be sent in accordance with the above periods.

Where consent has been given on a reciprocal basis (i.e where a customer can see that everyone on his/her locatable 'buddy list' can also locate him/her, only the first and the monthly reminders need be sent.

~~Alternative approach – frequency of location request~~

~~LSPs may choose algorithms for sending out randomised alerts that are based on frequency of location request rather than time based, as set out in the table below.~~

~~Period or frequency of request~~	~~Notification~~
~~Within first 24 hours of first consent being given~~	~~At least 1 SMS~~
~~1st request~~	~~At least 1 SMS~~
~~Next 6 requests~~	~~At least 1 SMS~~
~~Next 10 requests~~	~~At least 1 SMS~~
~~Every next twenty requests~~	~~At least 1 SMS~~

~~LSPs have the choice to use a hybrid of time based or request based alerts. For example, for the first month to use location requests as the trigger for the random alerts and thereafter to use time based alerts or vice versa. Alerts must be delivered at random, so that any potential miscreant cannot anticipate the timing of their arrival.~~

If the notification is not delivered, for whatever reason, it must be re-sent until it is delivered.

If the LSP receives no delivery receipt for the reminder SMS after 4 attempts or a maximum of 48 hours, the locatee must be suspended from the service. Before the locatee is reinstated on the service, a fresh consent must be obtained.

Random notifications to locatees must contain the following information:

- the service name;
- the notification must provide the individual with sufficient information to allow them to stop the service if they wish to do so; and
- website or customer support number where further service information including terms and conditions are available.

Note – the random alerts should be sent to the locatee in accordance with this schedule when consent is given for the first time. There is no requirement to repeat this schedule if the locatee consents to being located by additional locators on the same service.

As an example the following text may be sent to the locatee to remind them that a location service is still active:

"[You have consented to your phone being located through [SERIVCE NAME]. To stop this service please send STOP [SERVICE NAME] [NAME] to [SERVICE NUMBER]. [SERVICE WEBSITE] by [PROVIDER NAME]."]

If this message is not delivered, for whatever reason, it must be re-sent until it is delivered. Even if no location requests have been made in relation to a locatee since the previous alert was sent the alert must still be sent.

Service providers must provide a near real-time facility for the individual to view the name and phone number of all individuals that can locate them.

As an example the following text may be sent by the locatee:

"LIST [SERVICE NAME]" to [SERVICE NUMBER]

Service providers must provide an easily accessible facility to allow locatees to view, at least, the name, phone number date and time of the last 5 location request searches undertaken in respect of that locatee.

As an example the following text may be sent by the locatee:

"LIST LAST 5 [SERVICE NAME]" to [SERVICE NUMBER]

Note: There is no requirement to provide a near real time facility for Introduction/dating type services (ie where participants are not previously known to each other). Participants in these services must have been verified to be at least 18. The service provider must maintain a record of who can locate who and must, on request, be able to inform locatees who can locate them.

ANNEX E - Stopping, suspending service

It is strongly recommended that "STOP" be used as the command to stop a service either temporarily or permanently. "START" may be used to (re-)start a stopped or suspended service.

As an **example** the following text may be sent by the locatee as an SMS when de-activating a service which allows an individual to locate a child:

"STOP [SERVICE NAME] [NAME]" to [SERVICE NUMBER]

When de-activating all locators on a location service operated by a LSP:

"STOP [SERVICE NAME] ALL" to [SERVICE NUMBER]

Premium rate voice calls or premium SMS services should not be used for the de-activation of location services.

Where appropriate, LSPs should ensure that either:

- advisory messages are sent to the locator when a de-activation request is made by the locatee; or
- location status is available to locators to reflect a stopped or suspended service.
- The LSP will act on a “STOP” message on receipt.

ANNEX F - Location services and you

Location services work by identifying the physical location of a mobile phone or other mobile device. This could be your own mobile phone or the mobile phone of a relative, friend or work colleague.

A wide range of new services are possible using location services including telling you how to get to the nearest cash machine or chemist; allowing a parent to identify the location of his or her child; making it easier for friends to meet up for an evening out; and assisting firms with the security of lone workers.

All location services are subject to the legal requirements of the Data Protection Act. For consumers this means that location information can be used only after consent is provided by the user of the phone being located. For business users employers must explain to their employees how location information will be used before it is collected.

The Data Protection Act requires that customers are made aware of:

- who their location service company is;
- the purposes for which personal data - including location information - will be collected and processed;
- whether data will be sent to a third party for the purpose of providing the location service and length of time for processing data, including storage, will be.

In addition to data protection legislation, participants in the UK location services industry - including both location service providers and mobile phone operators - have agreed a Code of Practice for the provision of location services. This Code of Practice sets out additional requirements for different types of location services. This includes requirements relating to:

- registration of individuals and organisations using location information;
- provision of reminders on location services operating on a mobile phone;;
- how customers can stop a locating service which is running on their phone; and
- responsibilities of a locating business or other organisation.

While details vary, all location services depend on the **disclosure of where you are** to companies or to other individuals. This offers you significant opportunities to use new services. However, these services should be used with the same care as you would take in telling other people your location in a phone call or SMS. Further, unlike a phone call or SMS, they can provide information on your location over a period of time.

Only consent to the use of your location information if you would be willing to provide the same company or individual with details of where you are in a phone call or SMS. Be aware that your consent may apply for a period of time. Don't forget that you can withdraw your consent to being located at any time.

If you have any concerns about your safety which relate to the operation of any location service then you should contact your location service company.

If you have immediate safety concerns then you should, as in other circumstances, contact the police by dialling 999 or 112.

If a user of a location service believes that the industry Code of Practice are being breached by the location service provider, he or she may contact the Mobile Broadband Group by e-mail at mobilebg@btopenworld.com or write to The Secretariat, Mobile Broadband Group, PO Box 34586, London SE15 5YA.

ANNEX G - Extract from SI on Privacy and data protection

EXTRACT FROM STATUTORY INSTRUMENT – 2003 NO.2426 ELECTRONIC COMMUNICATIONS – THE PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS 2003

Restrictions on the processing of location data
14. - (1) This regulation shall not apply to the processing of traffic data.

(2) Location data relating to a user or subscriber of a public electronic communications network or a public electronic communications service may only be processed -

(a) where that user or subscriber cannot be identified from such data; or

(b) where necessary for the provision of a value added service, with the consent of that user or subscriber.

(3) Prior to obtaining the consent of the user or subscriber under paragraph (2)(b), the public communications provider in question must provide the following information to the user or subscriber to whom the data relate -

(a) the types of location data that will be processed;

(b) the purposes and duration of the processing of those data; and

(c) whether the data will be transmitted to a third party for the purpose of providing the value added service.

(4) A user or subscriber who has given his consent to the processing of data under paragraph (2)(b) shall -

(a) be able to withdraw such consent at any time, and

(b) in respect of each connection to the public electronic communications network in question or each transmission of a communication, be given the opportunity to withdraw such consent, using a simple means and free of charge.

(5) Processing of location data in accordance with this regulation shall -

(a) only be carried out by -

(i) the public communications provider in question;

(ii) the third party providing the value added service in question; or

(iii) a person acting under the authority of a person falling within (i) or (ii); and

(b) where the processing is carried out for the purposes of the provision of a value added service, be restricted to what is necessary for those purposes.

ANNEX H - Working Group participants

This Code of Practice has been complied for use by all location service providers. The working group compiling the Code of Practice has comprised of representatives from the following organisations:

3

Britannic 3G Services

Child Locate

Creativity Software

Follow Us

MI International

Mobile Commerce

Multimedia Messaging Systems/mTrack

MX Telecom

O2

Orange

Ordnance Survey

T-Mobile

Trackaphone

Vodafone