eNACSO European NGO Alliance for Child Safety Online

# The challenges posed by location services

## Introduction

The development of mobile phones and other portable devices has allowed for and encouraged the emergence of technologies which make it possible for an individual's whereabouts to be traced and tracked through their use of those devices. By pinpointing a mobile phone handset applications can show where someone is right now, where they were at a particular moment in the past, or show a record or pattern of their movements over a more or less extended period of time.

This type of information is potentially highly sensitive. Where it relates to a child it is even more so.

Location is an aspect of behaviour. Thus, in an online context, location data also raise potential concerns about behavioural advertising practices. Could location data be used deliberately to target and exploit young people? Could location data expose them, even unintentionally, to other risks?

### What is to be done?

In this paper we set out and draw on the UK experience with an earlier iteration of mobile phone based location services. Some of these were specifically designed to track children. However, the paper principally addresses the challenges posed by the very recent emergence of a new breed of location services. Inter alia, we argue that companies providing personal location data services should accept they are subject to a duty of care which goes way beyond the ordinary or the everyday.

### Surveillance society

In addition, in this paper we also ask whether or to what extent the new types of location services raise any fundamental or broader issues about the development of a "surveillance society", particularly if they start to become linked with other aspects of more modern mobile devices' functionality e.g. through geo-tagging?

There is a degree of urgency about this. Location applications are already out there actively recruiting new members and building market share. They are doing so free from any widely agreed standards.

### A self-regulatory initiative

Several leading global players in the mobile phone and location service space e.g. Google, Yahoo, Nokia, Vodafone, have come together to consider how to establish principles of best practice. The group was originally convened by Vodafone. eNACSO was invited to submit evidence to the group. This paper is a modified version of that submission.

## The UK experience of the first commercial location services

Vodafone, 02, T Mobile, and Orange are the largest mobile phone networks in the UK. In 2002/3 they started to roll out the first ever commercially available, mobile phone based, consumer-facing location services.

### How they worked

When someone turns on their mobile phone the SIM card within it links up to, or tries to link up to, the nearest available radio cell in the network of radio cells the subscriber's mobile phone company owns or operates. The physical location of each cell is known to the network operator. As a customer moves between cells the mobile network operator (mno) recognises and records that fact. Alternatively if a phone is turned off, runs out of power or goes out of range, the company knows the last place the phone was live. It was this data, derived wholly from the mobile phone networks, that formed the basis of the first location services. Such data is still used in some of the newer location services which are the principal subject of this paper.

### Accuracy

The level of accuracy with which the mno could determine a person's location or pattern of movement depended on a number of factors. The most important of these was and remains the number of radio cells within a particular area. In densely populated urban areas with a high number of radio cells the location data provided could be quite precise e.g. within 50-100 metres, whereas in rural areas with few network resources the location information then available could be very approximate e.g. to within a few square miles.

### Police and emergency service always had access

Prior to 2002/3 location information of this type had always been made available to the police on the production of an appropriate warrant, and it still is. The emergency services were also, and still are, allowed access to it in certain circumstances.

### Staring to sell location data to third parties

What changed in 2002/3 was the mobile phone companies found a way to monetise location data. They opened up a route to the mass consumer market. It changed everything.

## Two types of location services

At first there were two classes of location service: active and passive.

### Active location services

With active location services there are really only two parties: the handset user and the mobile phone network. The user had to initiate each and every transaction. For example someone might want to know where the nearest taxi rank is, or ATM, or Chinese restaurant, and they would in effect ask their mobile phone network to provide them with the answer. The mno knows which cell the mobile phone is in and has access to a database of a wide range of facilities close to or in that same cell. The mno simply cross references the two data sets and relays the information back to the handset user. The information flow was strictly two-way. We saw no major child protection issues in relation to this type of service. There are data protection and privacy concerns surrounding how the records of such location-related transactions are used or are stored by different parts of the value chain, but these are not specific to legal minors and neither, at the time we formulated the UK's code of practice, were we aware of any ways in which this type of data could put children at risk of exposure either to malevolent third parties or to inappropriate commercial or other entities.

### Passive location services

Passive location services are very different. They are principally about tracking people[1]. Here there are three parties to the transaction: the person doing the tracking (the tracker), the person being tracked (the "trackee") and the location service provider i.e. the company supplying the trackee's location data to the tracker. The tracker is the paying customer.

Typically the tracker e.g. a parent initiates the service. The trackee, the child, agrees to being tracked. Once this initial consent was given the trackee would normally have no knowledge of how many times or when the tracker had checked on their location. No further consents were required, hence the use of the term "passive".

The tracker would receive the location data via a web browser or it could be sent as a text message to a previously nominated number, or both. Potentially the information could also be sent as data to be picked up and utilised by other applications although in those early days we were not aware of any that did this.

In the UK it was the passive services which gave rise to major data protection, privacy and security concerns, particularly when a number of companies started promoting "child location services".

### Marketing child location services

The target market for child location services was parents and guardians. The subliminal, and in the early days sometimes the almost explicit marketing message was "Your children are in constant and imminent danger of getting seriously lost or even of being kidnapped. If you love your children and want to see them returned to you alive and well and quickly, you will buy our service. Moreover, and more generally, because you will always know where your children are, you will also always know they are safe."

### Flaws in the system quickly exposed

Several journalists from a number of UK national newspapers soon showed how easy it was to manipulate and misuse the new location services. They were able to track people without their knowledge or permission. These incidents received considerable publicity.

[1]Around the same time a significant market also developed for vehicle management or asset tracking in corporate markets. A discussion of these is outside the scope of this paper although it is acknowledged they can have raise personal privacy concerns, some of which could impact on the interests of minors.

### Mobile phone networks have a large stake

The mobile networks never sold location services directly into the consumer market. The services were marketed and provided by a series of small specialist companies that sprang up. These companies, in effect, became intermediaries. However, once stories started appearing in the mainstream media about major security breaches with the new location services the mobile phone networks got very engaged with the location companies. The networks wanted to make things safe for their customers but they also understood that if matters were not put right quickly it would be they, not the small location companies, that would suffer the real brand damage[2].

### The mobile phone industry decides to move

The mobile phone networks rapidly concluded that they needed to agree a set of common security standards. The networks expressly accepted the legitimacy of consumers' anxieties about location data and location based services, particularly services designed to track children.

The Mobile Broadband Group (MBG) is a UK industry body that brings together all the UK mobile phone networks, including the four companies that rolled out the first location services. The MBG was tasked to formulate, consult on and if necessary negotiate an industry wide code of practice on passive location services.

### Why had the mobile companies not foreseen these scenarios?

The only surprising and still unanswered aspect of this whole episode was why the mobile networks had not anticipated the scenarios which the children's organizations and the media so swiftly exposed.

[2] For similar reasons, in relation to the new location services which are the principal subject of this paper, the mobile phone networks have the same anxieties, and similar motivations for involving themselves in trying to determine any new standards that might be applied. However, it is also clear that as the mobile phone networks have themselves become or are becoming internet businesses, they are also keen to discover how they too can best exploit any commercial opportunities that the new location technologies might present.

## The UK code of practice for passive location services

Over a period of about twelve months a detailed code of practice on the operation and marketing of passive location services was developed. It became operative in September, 2004[3]. Similar codes or provisions were later adopted in other European countries as similar services started to be provided in those countries.

The precise status of the body that negotiated the UK code was always a little hazy but, from the perspective of the children's charities in the UK, it was a tri-partite negotiation. The parties were:

1. The MBG[4]
2. Law enforcement and Government[5]
3. The children's organizations[6]

### Main elements of the code

- Each trackee had to agree to being tracked by a specific individual.
- Typically this was done by an exchange of text messages between two nominated handsets, but in the case of child location services extra steps were also included (see below).
- The service was paid for so there was an audit trail linking back to a specific bank account or credit or debit card.
- Child location services could not be initiated wholly online. A password had to be sent through the post to a real world address. This password had to be given to the service provider (online) to begin the service.
- Doing it this way also meant the service could not be commenced immediately. Going through the post introduced a delay, an opportunity to reflect.
- Delivering the password to a real world address provided an additional audit trail and security check.
- The location company was required to send text messages to the trackee periodically reminding them their SIM card was capable of being tracked. These texts also explained how to halt the service. Typically this would simply be by sending a "STOP" message as a text to a given number. The code specified the frequency with which these reminders had to be sent to the trackee.
- Only a parent or legal guardian could initiate or give permission for a child to be tracked.
- Irrespective of their age, the child's consent was required to commence the service. Irrespective of their age, the child could indicate their withdrawal of consent at any time, normally simply by sending a "STOP" message, in which case the service halted straight away. There was no parental override.
- There were limits set in relation to how child location services could be advertised and promoted e.g. they must not play upon parents' unreasonable fears of their children being kidnapped or lost, nor should they suggest that simply knowing where your child's SIM card is is the same as knowing that your child is safe. For example the SIM card or the handset it was normally in, or both, might have been lost or stolen. Alternatively the child might have the handset and SIM card in their possession but nonetheless still be in a perilous situation.

[3] http://tinyurl.com/yb9e6nq

[4] The MBG also brought in a number of location service suppliers – the companies they were providing the location data to and who were, in turn, marketing it to the public. The location companies sat alongside the networks in the negotiations.

[5] As represented by the Association of Chief Police Officers and the Home Office

[6] As represented by CHIS, the Children's Charities' Coalition on Internet Safety (www.chis.org.uk)

- A child's location data could not be broadcast to groups of people or to public or semi-public places. It was always one to one.

- Finally, regular audits of the operation of the code were required. The results of the audits were reported back to meetings of all the parties who had been involved in negotiating it. These meetings were convened by civil servants from what is now the Ministry of Justice.

### What was not included in the code

The children's charities would have preferred the code to go further in several respects

- ✓ to require the trackee's consent each time location data was requested i.e. before the data could be transmitted to the tracker.

- ✓ that a log be kept and regularly sent to the trackee and their parent or guardian showing when and by whom location data had been requested.

- ✓ the audit of the operation of the location services should be carried out by an independent entity, not by the companies themselves.

The industry would not agree to any of these items. They were not included in the code.

### Advertising and marketing issues were not then to the fore

Before the discussions on the code started, to a limited extent we had already seen a form of location data being exploited for commercial purposes. Bluetooth was being used to serve advertisements to mobile phone users. Advertisements were being transmitted to people's Bluetooth enabled devices as they walked by or near a shop or restaurant that wanted to entice them in. Strictly-speaking, a very high proportion of the advertisements must have been spam.

The potential for other forms of location data to be used on a much larger scale by commercial or other concerns was therefore raised in the course of the discussions on the UK code. However, no provisions were included in the code in relation to that aspect. It was then still little understood. The matter was "parked". We knew we would have to return to it at a later date. That later date seems now to have arrived.

## The new breed of location services

A new breed of location services is emerging. As with the original services they provide the possibility of tracing either a person's current location or, depending on the application, they can show where a person was at a given time in the past or show a record of an individual's pattern of movements, stretching back hours, days, months or even longer. However, the level of accuracy which can be achieved by the new services is significantly greater than the original services. Some of the new services can locate a person in either a built-up or a rural environment to within a matter of a few feet.

### The role of the internet

The new services principally operate over the internet utilising detailed maps or other kinds of relevant location based information, through a form of location "handshake" with the mobile handset.

The location data which can be supplied to the new location service providers could come from:

- Mobile phone cells e.g. via Open Cell ID
- Satellite, via the Global Positioning System (GPS)
- Mapping wifi hotspots e.g. via Skyhook
- Some permutation of the above[7]

As with the original UK services some of the new breed of location services are being used for vehicle management or asset tracking in corporate markets, but many are moving quickly towards "friend finder", social networking or other people-focused services or markets. In some of these markets legal minors are to be found in very large numbers.

### Data protection laws

Whilst we can all probably feel confident the large operator licensees will work within every country's data protection and privacy laws, typically by always following the principle of requiring customers to "opt in" to location services, these principles may be challenged by international and creative companies who are innovating at the edge of the networks, or who have less understanding of the opt in arrangements that should apply. Like the myriad apps that have appeared for mobile phones, the new location applications are being invented or developed by some extremely small companies based all over and anywhere in the world.

### No controls?

At the moment it seems most of the handset manufacturers, mobile phone network operators and web site owners with an interest feel powerless to act in this space because they do not have the technical mechanisms for blocking or controlling the deployment of the new location applications. This in turn means that both highly innovative data sharing applications and sometimes completely rogue location applications could find their way into the ecosystem to obtain and exploit people's location data in ways which might be dangerous, unlawful or both.

### Apple acts as a gatekeeper

Apple seems to be one of the few companies, perhaps it is the only company that has found a way of dealing with this latter problem. Through its "Apps Store" Apple must approve all applications before they can operate via their technology. As yet no other handset manufacturers appear to have established a similar capability.

[7] The hybrid systems will generally be the most accurate and fastest.

## Wider concerns

A consideration of the issues surrounding the new location services is further complicated by the potential for some or all of the functionalities of the newer mobile handsets to become linked to location services.

### Electronic eavesdropping and remote video surveillance

Certain phones can be turned into remote listening devices by the simple expedient of sending an inaudible text message which automatically turns on the device, allowing the person at the other end to eavesdrop third party conversations. In like manner some handsets can be turned into remote video cameras, this time with a combined audio and video function.

### Linking pictures and sound to location data

If real time (or historic) data also becomes available showing the physical location of the conversations being listened to or the videos being watched, the potential for harm or mischief is that much greater. With geo-tagging we are already seeing the beginnings of this type of crossover application.

### An electronic leash for children

Some services can send a text message or an email to a specified address or number whenever the nominated handset goes outside a previously defined geographical perimeter. These have been incorporated into a number of child location services. The phone in effect becomes an electronic leash for the child. Potentially this may be valuable in a very limited number of circumstances but as an everyday feature of parenting it implies a lack of trust or confidence in a child that could be truly corrosive of healthy family relationships. It suggests other or underlying issues which ought to be addressed.

### More James Bond than mobile phone

Taken together, mobile phones are beginning to look less and less like useful personal communicators and more and more like instruments of electronic control, or even espionage.

### Surveillance society

It is not hard to see where this broader debate might end up. Amidst broader discussions about the development of a "surveillance society", it will not be just the children's organizations that raise concerns. Developments of the kind being discussed here have the potential to construct a very broad alliance of otherwise disparate groupings of socially engaged citizens, not to mention the political parties. Within such an alliance the children's organizations would be a relatively small part, although undoubtedly the children's angle could well be the one the mass media home in on.

### The original location services are dying out

The original location services still exist in the UK and elsewhere, but it is probably already the case that the majority of location services operating in most of Europe are being provided over the internet by companies that do not regard themselves as being bound by the terms of the UK code or any of its equivalents elsewhere. Those codes are dead, dying or irrelevant. The emergence and convergence of social networking, behavioural advertising and other online technologies are challenging many different aspects of data privacy in the 21st century. Location is only one part of that larger story, albeit one of key importance.

## Problems with the new breed of location services

The potential advantages of location services are obvious, but so are the potential downsides:

- Because the new location services can be linked to social networking sites and other online services, a major concern is that, without fully understanding the potential consequences, minors are publishing or will soon start to publish location data about themselves as part of their profile.

- The risk of this happening is rooted in the very simple and obvious fact that whilst most location service providers may specify 18 as the minimum age for users of their service, none have developed any effective means of enforcing or policing this.

- In addition most web sites that a location service might be deployed to e.g. a social networking site tend to specify 13 as the qualifying age. We leave on one side for now the knowledge that children several years short of their 13th birthday are also very active on all parts of the internet. We have little doubt that sub-13 year olds will also be able to access location based services.

- Children and young people who have been loose or careless with the number of people they have accepted as "friends" could, in effect, be creating a new type of passive location service. This means that, absent any countervailing measures, neither the young people themselves, nor their parents or guardians, will have any way of knowing who is checking on their whereabouts or when. Location data will be broadcast to perhaps thousands of people whom they do not know in any meaningful sense. This echoes concerns of a similar nature about other aspects of children's personal data being published on social networking and other sites, but adding location data into that same mix potentially magnifies those risks or it constitutes an entirely new one.

- One of the key reasons the problems being discussed here arise at all, certainly as compared with the original location services in the UK and other European countries, is because predominantly the new breed of location services are being provided "free" to the end user. This makes it a lot easier for minors to sign up for and use the services. People will wonder whether "free" is a price worth paying.

- Because location services are being financed through advertising and are not being paid for by the end user, a potential audit trail and several checks or deterrents to underage use or third-party misuse are lost.

- Almost by definition the advertising activity that will finance the services will be directed at adult audiences. It is therefore likely that if children and young people are in and around location applications they may frequently be exposed to promotions of age inappropriate products and services e.g. alcohol, tobacco, gambling, which they could not anyway buy legally.

- Notwithstanding the risk of minors being exposed to age inappropriate advertising, there remains the possibility that a young person's location data could be used to provide the basis for serving advertisements for a range of products or services which they could legally buy. Yet they may never have given, or been legally capable of giving, informed consent to receiving such advertising.

- It should also be noted that it may not be only commercial concerns that could use location data in inappropriate ways to target children and young people. Other organizations could do so as well.

- Countless pieces of research have shown that significant numbers of young people persistently act very unwisely in a number of online environments, putting themselves and sometimes others at risk. Any company stepping into or remaining in the location market cannot plead ignorance of this dimension. Equally web sites which allow other companies' location applications to operate in their environment cannot escape responsibility for the consequences of that decision.

- Some location service providers might wish to say "So this is all about children telling lies about their age to get into areas or get to use services they shouldn't, or it's about them behaving badly or stupidly online. These are problems that are endemic to the internet as a whole. They are not special to us." But few other online services deal solely or routinely with information which is as sensitive as location data. Companies dealing with location data should be held to a higher standard. They have a special duty of care which is grounded in the nature of the information they are handling.

- If the service can be initiated wholly online, and immediately, it will allow for more impulsive forms of behaviour. Children and young people are more prone to impulsive behaviours.

- A key concept in most data protection laws is that the person "opts in" to a specific service, giving consent to a particular proposition. The person should therefore understand, if not absolutely everything about the service, then at least its key terms. This implies that all the important relevant information about the service is presented at sign up, and is readily comprehensible.

- It is doubtful this is happening now, even when an adult of average intelligence and average levels of literacy and numeracy is initiating a service on devices with standard size computer screens. The internet is not a medium which easily allows one to absorb dense, often obscure, lengthy legal language. It must truly be open to doubt that this fiction can be maintained when a service or subscription is being initiated using screens such as those found on most mobile phones and similar small form factor devices. With minors the challenge is that much greater again, irrespective of the size of the screen being used.

- Taken together, all these different developments may well reopen a debate around age verification. This time it will be in a rather different context from that which prevailed in the USA in 2008/9 where it was raised by the Attorneys General in relation to social networking sites. In that case age verification was put forward as a way of "guaranteeing" adults could not find their way into online environments intended principally or exclusively for minors. The subsequent study by the Berkman Center of Harvard University[8] showed how problematic that notion was.

- In the context of a discussion on location services, however, robust age verification could be proposed as a means of preventing minors from joining a service which is specifically limited to persons aged 18 or above. The UK and other countries have well developed reliable online systems which allow a web site owner very easily, quickly and inexpensively to determine online in real time whether or not someone is legally an adult[9].

The complexities of dealing with this issue clearly are substantial. But just because technology has evolved to a point where these new types of location applications are possible, it does not mean they are inevitable. Much less does it mean that society must accept them as they are now. Such services could be curtailed altogether if they are seen to have hugely unacceptable consequences or risks attaching to them.

[8] http://cyber.law.harvard.edu/research/isttf

[9] In the UK it is a condition of obtaining a licence to operate an online gambling web site that the operator has an online age verification system in place. The minimum age for gambling, online and off, is 18.

## What does eNACSO want?

- A new code of practice on location services is needed. It should seek as far as possible to replicate and add to the security provisions of the original UK code, particularly in relation to child location services.

- Any new code should apply at least EU-wide, or on a larger basis if possible.

- By default, location services should be classified as an adult service.[10]

- The new code should specify that only persons aged 18 or above may be the subject of a location service or may initiate one, unless the verified consent of a parent or guardian has been obtained. Robust verification systems should be developed in order to underpin this policy.

- In addition, recognising that minors will obtain parental consent to be the subject of a location service, or be the initiator of such a service, the new code should also contain provisions in relation to how minors' location data might be used and by whom e.g. in relation to targeted marketing, behavioural advertising or other activities.

- Location data about minors should not be broadcast to any kind of public group or to any web page which can be found by any search engine.

- Location data about a minor should only be visible to individuals who have logged in to a particular web page specifically to request it[11].

- Establishing appropriate audit trails should be investigated e.g. with notice, recording the IP addresses and log in details of everyone who uses a web site to view location data about a minor.

- Before any third party can track a child he or she must be approved both by the child and by their parent or guardian. Consent can be withdrawn at any time by any of these parties. Withdrawal of consent by any party will bring the service to an end forthwith.

- Where the minimum age stipulated by a location service provider is 18, no one registered as being under that age with another site should be able to run the service on that site unless verified parental consent has been obtained by the receiving site.

- No location application should be able to work on any handset or other internet enabled device, or on a web site, unless and until it has been authorised and approved by an appropriate standards body, perhaps in the manner of an "Apps Store".

- Hardware manufacturers, mobile phone networks and other relevant interests need to be engaged to see what they can do to underpin this policy e.g. by limiting the potential for location data to be "picked up" by any applications that have not been through a recognised approval process.

- Location service providers should be required to keep a log of every request for location data that is made in relation to a minor, for this log to be visible at all times to the trackee and to their parent or guardian and for it to be automatically forwarded to each of them at appropriate intervals.

- Hardware manufacturers should ensure that whenever a location application is running or the device is broadcasting any kind of location data that is capable of being picked up by applications running on

[10] In several European countries the mobile phone companies put gambling, pornography and similar age sensitive services behind an adult bar by default. Different companies have different ways of allowing the adult bar to be lifted but in each case it involves the user proving they are over 18.

[11] In a school or similar setting, and for clearly defined time limited purposes e.g. a field trip, it should be possible to vary this otherwise necessarily strict requirement.

the handset or running externally to the handset, an icon flashes on the screen constantly to remind the handset user of that fact.

- Ideally the apps providers also would be required to do something similar but the hardware manufacturers should be able to create and embed something in the device itself which is turned on by default as a guarantee or as a fallback

---ooo---

John Carr
eNACSO Board Member
14th March, 2010

John.carr49@btinternet.com
www.enacso.eu