

Summary

Information about a person's physical whereabouts is sensitive. Where the information relates to the physical whereabouts of a child, it becomes doubly sensitive, particularly if it is rendered in real time, or near real time.

In the UK the legitimacy of these concerns was accepted by the mobile phone network operators in 2003 when they began to roll out the first ever commercially available consumer-facing location services. Some were specifically marketed as "child location services".

A self-regulatory code of practice governing the operation of location services was established. It became operative in September 2004. Compared with location services for adults, extra layers of security were built in to the child location services. Provisions broadly similar to those adopted in the UK code were later followed in other countries that also rolled out location services.

However, the technology has moved on. A new breed of location services has started to emerge. These services operate largely via the internet using data which are outside the ownership or control of the mobile phone networks. The applications that collect and utilise the data similarly may require no prior approval or authorisation by any of the established mobile or internet gatekeepers. The original UK and similar codes are now obsolete or at best obsolescent.

What safeguards are needed to ensure that children and young people are not put in danger from their naive or unauthorised use of some or all of the new location services? Do these new location services raise any broader issues about the development of a "surveillance society"?

It is readily acknowledged that the technical challenges presented by the new breed of location services are formidable. Key players in the internet and mobile phone industries across the EU have come together to try to develop a self-regulatory response that will meet legitimate consumer and child protection concerns. eNACSO is pleased to be part of those discussions and this paper represents its first input to them.

John Carr
eNACSO Board Member

July, 2009.

Early UK experience of location services

The UK saw the first roll out of large scale, commercially available mobile phone based consumer-facing location services. This was around 2003. The (typically) small companies that were selling these services depended wholly on data supplied to them by the mobile phone network operators. That data could be viewed or accessed, and a location could be determined, either via a web browser or as a text message sent to a mobile handset, or both.

As the then sole source of the location data the mobile phone networks had considerable power to determine the standards the location data suppliers had to follow. If the location companies did not comply, they were simply cut off and effectively put out of business.

As the services developed, the mobile networks got very engaged with the location companies. In part this was because the networks knew, if anything went wrong, it would be they who would suffer the most brand damage. Research continues to show that whenever anything “bad” happens via a mobile phone handset many consumers will blame or look to their mobile phone network operator to put it right or to compensate them for it. This is rooted at least in part in the fact that the consumer has a billing relationship with the network and therefore seemingly feels the network has a responsibility for everything that happens to them whilst using it.

No doubt in the current discussions concerning the newer forms of location services, the mobile phone networks have similar anxieties and therefore similar motivations for involving themselves. However, it is also clear that, as the mobile phone networks have become or are becoming internet businesses themselves, they are also keen to discover how they too can best exploit any commercial opportunities that the new location technologies might present.

The original location services

In the beginning there were two classes of location service: active and passive.

With active location services there were really only two parties: the handset user and the mobile phone network. The handset user was always in control. The user had to initiate each and every transaction. For example they might want to know where the nearest taxi rank is, or ATM, and they would in effect ask their mobile phone network to provide them with the answer. The information flow was only two way. We saw no major child protection issues in relation to this class of services. There were data protection concerns surrounding how the records of such location-related transactions were used or stored by different parts of the value chain, but these were not specific to legal minors.

Passive location services were principally about tracking people¹. There were three parties: the person doing the tracking (the tracker), the person being tracked (the “trackee”), and the network supplying the trackee’s location data to the tracker. Typically the tracker e.g. a parent, would initiate the service, the trackee would agree to being tracked, but after that the trackee would have no knowledge of how many times or when the tracker checked on their location. The trackee gave their consent at the beginning and thereafter they were not required to do anything or to consent further, hence the use of the term “passive”.

¹ Although using the same technology a large area of activity also grew up around tracking vehicles or goods.

It was the passive services which gave rise to data protection, privacy and security concerns, particularly when a number of companies sprang up promoting and selling “child location services”. Their target market 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 of being kidnapped. If you love your children and want to see them returned to you alive and well 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.”

Several journalists from several national newspapers soon showed how easy it was to manipulate the first tranche of services. They were able to track third parties without their knowledge or permission. Amongst other things these incidents underlined the importance of the mobile phone networks agreeing a number of basic standards, particularly in relation to the child location services. The UK’s code of practice was the result.

The code 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 negotiated. It became operative in September, 2004.

The code set out various measures which had to be taken to minimise the possibility of the service being abused.

The precise status of the body that negotiated the original 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 mobile phone industry, represented by the Mobile Broadband Group and a small number of location service suppliers whom they brought in alongside them;
2. Law enforcement and Government, as represented by the Home Office and ACPO;
3. The children’s organizations, as represented by CHIS.

The code that was finally adopted was reported to and noted by the Home Office Task Force. The code provided for audit and review meetings. These were convened by civil servants who were then in the Home Office and are now in the Ministry of Justice.

Main elements of the code

1. Each trackee had to agree to being tracked by a specific individual.
2. In general this was done by an exchange of text messages between two handsets, but in the case of child location services extra steps were also included (see below).
3. The service was paid for, so there was the comfort of an audit trail linking back to a specific bank account or credit card.
4. In the case of a child, the process could not be completed wholly online. This meant that neither could the service be commenced immediately. A code was sent through the post. This code had to be utilised to commence the service.
5. Having the code delivered to a real world address meant there was an additional audit trail and security check built in.
6. There were requirements in relation to the frequency of text messages being sent to remind the user that the SIM card in that handset was capable of being tracked. These texts also reminded the trackee how they could stop the service.

7. In relation to a child location service the tracker had to declare what their relationship was to the trackee, and only a parent or legal guardian could properly initiate or give permission for a child to be tracked.
8. There were limits set in relation to how child location services could be advertised and promoted e.g. they must not play upon parents' fears of their children being kidnapped, nor should they suggest that knowing where your child's SIM card might be is the same as knowing that your child is safe.
9. Irrespective of their age, the child's consent was required to commence the service and, again irrespective of their age, the child could indicate their withdrawal of consent at any time, in which case the service stopped immediately. There was no parental override.
10. There was no question, at least in respect of children, of a person's location data being broadcast to groups of people or to public or semi-public places. It was always one to one.
11. Finally, in respect of children's services regular audits were required and, as noted above, these were reported back to a joint meeting of Government, law enforcement, the industry and children's charities.

What was not included

The children's charities would have preferred the code to go further in some respects e.g. to require prior consent each time location data was requested and before it could be transmitted to the tracker; that a log be kept and regularly sent to the trackee showing when and by whom location data had been requested and that the audit of the service be carried out by an independent agency. The industry would not agree to any of these items. They were not included in the final code.

The new breed of services

As already noted, there is now a new breed of location services. These operate over the internet. The location data which can be rendered to a location data service provider can come from one or more sources, all of which are outside the control of the mobile phone network operator, namely:

1. via GPS
2. via Open Cell ID
3. via the mapping of wifi hotspots
4. via some permutation of the above

Secondly, the applications which can collect and utilise this data typically work through standard APIs or open source code. This can mean that mobile phone handset manufacturers, mobile phone network operators and web site owners do not necessarily always have a technical mechanism for blocking or controlling deployment of such applications. Apple has an "Apps Store" which means it can exercise some control of applications which operate via the iPhone, but as yet no other handset manufacturers appear to have a comparable mechanism.

The original location services still exist, but it is probably already the case that the majority of personal location data services operating in the UK and other parts of Europe are being provided by companies that do not regard themselves as being bound by the terms of the UK code or any equivalents elsewhere.

Wider concerns

A consideration of these issues may be further complicated by the potential for some of the functionalities of the newer mobile handsets to become linked to location services.

Some 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. Some handsets similarly can be turned into remote video cameras, this time with a combined audio and video function. If real time (or historic) data also becomes available showing the physical location of the conversations being listened to or the videos being watched then the potential for harm or mischief is that much greater.

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

It is not hard to see where this debate might end up. Amidst broader discussions about the "surveillance society", it will not be just the children's organizations that start getting agitated. Developments of the kind being discussed here have the potential to construct a very broad alliance of otherwise disparate groupings of socially concerned 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.

Problems with the new breed of location services

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

1. Because they are paid for by advertising, typically no payment mechanism will be used to initiate the service. This means that one key audit trail is lost.
2. If the services can be initiated wholly online without, for example, having to send codes to real world addresses, that eliminates a further security check and audit trail.
3. Precisely because these services will be free to the end user, absent any countervailing measures, it must be anticipated that legal minors will access and use them.
4. If the services can be initiated wholly online it also allows for more impulsive forms of behaviour. Children and young people are more likely to be prone to impulsive behaviour.
5. It is acknowledged that some or all of the location service providers might stipulate a minimum age for persons to use their services e.g. 18, but absent any additional steps they have no way of actually knowing if their end users are, in fact, 18.
6. Web services which allow location services to be used on their sites, or are powerless to prevent them from being used on their sites, may have different and lower age thresholds e.g. Fire Eagle specifies 18 as their minimum age, but Twitter and many social networking sites stipulate 13 as their entry level.
7. Not all of the new breed of location service will work in the same way but there already are some which allow a person, in effect, to broadcast frequently updated real time information about their current location to many different web sites. The concern here is that any children and young people who have been loose or careless with the number of people they have accepted, for example as "friends" on their social networking site, will in effect be creating a passive location service where their location data is being indiscriminately

distributed to perhaps thousands of people whom they do not know in any meaningful sense of the word.

8. At this point some suppliers of location services might say "Ah, so it's not our problem. This is about media literacy. This is about children telling lies about their age. This is a problem which is endemic to the internet as a whole and it is not special to us." That argument will not run very far or for very long. Few if any other companies are providing such sensitive information that has the potential to produce catastrophic results so immediately.
9. Social networking and other web sites, as well as Governments and schools across the world, are spending millions and millions of pounds and thousands of hours talking about good netiquette and responsible behaviour online, precisely because it is well known that substantial numbers of children and young people persistently get these things wrong. Any company stepping into the location market place must know or anticipate that, absent any countervailing measures, they will be allowing minors to access and use their services. This will create issues not only for the companies running the location services, but also for the web sites that allow such services to link to them or are powerless to prevent them so doing.
10. A key concept in UK data protection law is that the person giving consent to a particular proposition must properly understand all of the key terms. This implies that all the important relevant information about the terms is presented at sign up, and the information is comprehensible and accessible. It is doubtful if that is happening now, even when people are initiating some services on devices with larger screens, but it must truly be open to doubt that this fiction can be maintained when the service is being initiated on the size of screens found on mobile phones and similar small form factor devices.
11. These developments may well reopen a debate around age verification, but this time in a rather different context i.e. it will not be about the potential value of age verification as a means of screening- out potential sexual predators, or of creating environments which are "guaranteed" to contain only persons of a certain age. It will be about age verification as a mechanism to prevent children putting themselves at risk by exposing information about their physical whereabouts to people who are, for practical purposes, complete strangers.

The complexities of dealing with this issue clearly are horrendous. That much is obvious, but just because something is technically possible it does not mean that it must happen, should happen or cannot be rolled back if it happens and has hugely unacceptable social consequences or risks attaching to it.

What does eNACSO want?

A new EU-wide code is needed which, as far as it can, replicates the provisions of the UK's original code and any similar codes developed elsewhere.

Ideally no location application should be able to work on any web site unless it has been authorised and confirmed by a standards body or trusted brand and is accepted by the web site owner as meeting certain basic standards, in the manner of an "Apps Store". Perhaps the W3C could help?

At least one major location service provider, Yahoo's Fire Eagle, has specified that only persons aged 18 or above may join. We endorse this view, although please note our earlier comments about the weakness of this position in an environment where no reliable age verification mechanism exists and no other mechanism is involved which would create a reliable audit trail.

The potential disjuncture between the minimum age stipulated by the location service provider and web sites allowing such services to be used is an obvious point that needs to be addressed e.g. if someone is registered with a site as being 14 it should not be possible for them to use a service on that site that is specifically intended for those aged 18 or above. Both the location service provider and the hosting web site should address this e.g. could Fire Eagle disable their service from working on non-compliant web sites, or withdraw permission for it to be used on such sites?

Alternatively if any web site allows a person who is registered with them as under the age of 18 also allows them to run a location service on their site, it must first obtain verified parental consent.

All or most of Europe's mobile phone network operators have data on whether their customers are registered as legal minors. A way should be found to tie that data into the use of these types of services i.e. anyone registered as sub-18 with a mobile operator should not be able to use a location service on their handset (unless a parent has given express, verified consent). That suggests all location services go behind an adult bar.

For anyone to have the ability to track a child they must have been individually approved, both by the child and by their parent or guardian. It should not be possible for a minor to broadcast their location data to any kind of public group. It should always be visible only to individuals and only after they have logged-in. Perhaps in order to check a person's location data the tracker must be required to log in to a specific part of the web site so the fact that Mr Bad Person had looked at Ms Thoughtless Child's location data is recorded somewhere?

Other potential security measures ought to be explored e.g. alternative audit trails (capture the IP address of everyone who logged in to look at a page containing location data?), delays in activating the service, the use of codes both to activate and use the service each time.

The handset manufacturers need to be engaged to see what they can do to limit a handset's capability to broadcast location data, either by default or at all. Perhaps the manufacturers could be prevailed upon to ensure that whenever a location application is being used on their device an icon flashes on the screen constantly to remind the handset user of that fact.

---000---