European NGO Alliance for Child Safety Online

Submission to the W3C Privacy Workshop

Child protection concerns and the new location services

Summary

Information about a person's physical whereabouts is sensitive. Where that information relates to the physical whereabouts of a child it becomes doubly sensitive. This is particularly true if the location data is rendered in real time, or near real time, but it applies equally to historic data which show or reveal patterns of movement.

In 2003 in the UK the mobile phone network operators began to roll out the first ever commercially available consumer-facing location services. Some of these were specifically targeted at parents and marketed as "child location services".

The legitimacy of people's concerns about making personal location data available to third parties was accepted straight away by the mobile phone network operators. The legitimacy of people's particular or extra concerns about children's location data was also acknowledged by the networks.

A self-regulatory code of practice governing the operation of location services was negotiated. It became operative in the UK in September 2004. The code made provisions in relation to all types of personal location services but additional layers of security were built in where the service was specifically intended to track children. Measures which were broadly similar to those in the UK's code were adopted in other EU countries when similar services were rolled out a little later.

However, the technology has moved on. A new breed of location services has started to emerge. Some refer to them as "Location 2.0". These services operate largely via the internet using data which are outside the ownership or control of the mobile phone networks. Most of the applications that collect and utilise the data similarly, at the moment, require no prior approval or authorisation by any of the established mobile or internet gatekeepers. They utilise standard APIs and open source code, interfacing with a range of different hardware components which are built into phones, laptops and other internet enabled devices.

Key players in the internet and mobile phone industries across the EU, and indeed now more widely than that, have come together to try to develop a self-regulatory code or response that will meet legitimate child protection and wider consumer concerns about the privacy and security aspects of the new location services. eNACSO was pleased to be part of those initial discussions and this paper is a slightly modified version of our input to them.

Our question to the W3C Privacy Workshop is simple: can you help?

John Carr
May, 2010
john.carr49@btinternet.com

The original location services in the UK

The roll out of commercially available mobile phone based consumer-facing location services began in the UK in 2003. The companies that sprang up to sell these services depended wholly on data supplied to them by the mobile phone network operators.

Originally there were two classes of location service: active and passive. Active services generally involved only two parties: the end user and the network. Passive location services necessarily involved at least three parties. They were principally about tracking people[1]. Passive location services gave rise to major data protection, privacy and security concerns, particularly when a number of companies sprang up promoting and selling "child location services".

The Mobile Broadband Group (MBG), an industry body, initiated discussions on the development of a code of practice to address parental and wider consumer concerns about the new services.

The code of practice

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[2]. Other countries adopted similar codes as the same services started to be rolled out there as well.

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

1. The MBG. The MBG also brought in a small number of location service suppliers to sit alongside them in the negotiations.
2. Law enforcement and Government, as represented by ACPO[3] and the Home Office;
3. The children's organizations, as represented by CHIS[4].

Main elements of the code

1. Each person to be tracked ("the trackee") had to agree to be 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 an audit trail linking back to a specific bank account or credit card.
4. Child location services could not be initiated wholly online. This meant the service could not be commenced immediately. 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.
5. Having the password delivered to a real world address meant there was an additional audit trail and security check built in.
6. The location company had to send text messages to the trackee reminding them that the SIM card in that handset was capable of being tracked. These texts also explained how to halt the service. The code specified the frequency at which these reminders had to be sent.

[1] Although a large area of commercial activity also grew up around tracking vehicles or goods.

[2] **http://tinyurl.com/yb9e6ng**

[3] Association of Chief Police Officers

[4] Children's Charities' Coalition on Internet Safety (www.chis.org.uk)

7. Only a parent or legal guardian could 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' unreasonable 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, 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 the code in the first place. These meetings were called and clerked by civil servants from the Ministry of Justice.

What was not included

The children's charities would have preferred the code to go further e.g. to require the trackee's prior consent each time, before any location data 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 the audit of the operation of the services should be carried out by an independent agency. The industry would not agree to any of these. They were not included.

Problems with the new breed of location services

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

1. Typically the new breed of service is supported by advertising. A payment mechanism will not be used or required to initiate the service. A key security check and audit trail is lost.
2. If the services can be initiated wholly online without, for example, first having to send a password to a real world address, a second security check is lost.
3. 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.
4. Because these services will be "free" to the end user it must be anticipated there is a greater potential for improper use generally, as there is with all "free" services. But companies dealing with location data should be held to a higher standard. They have a special duty of care which is grounded in the type of information they are handling.
5. Internet companies, Governments and schools across the world are spending millions of pounds and thousands of hours talking about online behaviour precisely because it is well known that substantial numbers of children and young people persistently get these things wrong e.g. they lie about their age or, on their social networking site for example, they are very undiscriminating about whom they accept as "friends". Any company stepping into the location services market place must therefore know or anticipate that, absent any countervailing measures, they will be allowing minors to access and use their services[5]. This will create issues not only for the companies running the location services, but perhaps also for any sites that allow them to link to them or are powerless to prevent them.

[5] It should also be noted that while services such as Fire Eagle might specify 18 as their minimum age, Twitter and many social networking or other sites they can link to stipulate 13 as their entry level.

6. Some location service providers might say “So this is about children telling lies about their age, a problem which is endemic to the internet as a whole. It is not special to us.” But few other online services deal with information which is as sensitive as location data.
7. The UK’s statutory telecoms regulator, OFCOM, has established that 25% of children between the ages of 8 and 12 have a profile on a social networking site, despite the fact that in the majority of cases 13 is the designated minimum age[6]. These sites clearly have no effective means of policing their age limits, and neither have the suppliers of location services. Yet despite this widely acknowledged failure, into this volatile mix has been dropped location services which add a wholly new and additional set of security risks.
8. The concern is, for example, that children and young people who have been loose or careless with the number of people they have accepted as “friends” on their social networking site, if they choose to link a location service to their profile, will in effect be creating a new type of passive location service where their location data is being distributed to perhaps thousands of people whom they do not know in any meaningful sense of the word. That could be a source of great risks of various kinds.
9. Location is a key aspect of behaviour and behavioural advertising could exploit children’s and young people’s naiveté or expose them to age inappropriate advertising.
10. A key concept in many countries’ data protection law is that the person giving consent to a particular proposition should understand its terms. This implies that all the important relevant information is presented at sign up, and is readily comprehensible. It is doubtful if that is happening now, even when people are initiating 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 using screens such as those found on most mobile phones and similar small form factor devices. If a child or young person is also able to initiate the service the difficulties in this respect are even greater.
11. Although some of the new location services, as with the original UK ones, regularly send reminders to users, telling them that they are broadcasting location data, this is unlikely to be much help with some children and young person who initiated a service, in the first place, in part by lying about their age and getting away with it.
12. 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 age verification as a means of screening- out potential sexual predators, or of creating environments which are “guaranteed” to contain only persons below 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 all practical purposes, complete strangers.

What does eNACSO want?

It would be very good to know from the W3C Workshop on Privacy if

(a) Members accept the legitimacy of the concerns expressed here
(b) Members could indicate what, if anything, is possible at a technical level to support or underpin some or all of the measures or policies we are advocating

Our view is that a new code of practice is needed which, as far as it can, replicates the provisions of the UK’s original code. This code should apply at least EU-wide, or on a larger basis if possible.

Ideally no location application should be able to work on any equipment or web site unless and until it has been authorised by a standards body or trusted brand, perhaps in the manner of an “Apps

[6] http://tiny.cc/ofcomnumbers

Store". This would in effect turn the "Apps Stores" or their equivalents into gatekeepers. No doubt part of the approval process would also entail ensuring that the apps provider is only able to collect the minimum information needed to make the service work, and nothing more.

18 should be established as the minimum age for any and all location services i.e. no one under the age of 18 should be able to make themselves a subject of a location service unless the location service provider has obtained verified parental consent. If the provider is not willing to go to the trouble of obtaining verified consent it should not allow minors to be the subject of their service.

A working system of age verification should be developed and integrated into the services to help ensure that persons below the age of 18 are not able to make themselves the subject of a location service without parental consent. The example of the UK's online gambling industry is commended to your attention.

In relation to mobile phone networks, location services should be classified as an adult service and put behind the adult bar. Within the mobile companies' filtering servicea for the internet, location service companies' web sites should be put behind the adult bar[7].

Any potential age disjuncture needs to be addressed e.g. where the minimum age stipulated by a location service provider is 18, and a third party web site knows that its customer is, say, 14, the site should be able to prevent the 14 year old from using a location service, again unless and until verified parental consent has been obtained.

It should not be possible for a minor to broadcast their location data to any kind of public group. Location data about a minor should only be visible to individuals and only after the individual has logged-in. Perhaps in order to check a person's location data the tracker should 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. to become a tracker of a child, the tracker must be individually approved, both by the child and by their parent or guardian. Absent any credit card or similar reliable data, alternative audit trails are needed. Maybe capture the IP address of everyone who logs in to look at a page containing location data? Should there be delays in activating the service, with passwords required to activate and/or 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? Ideally the apps provider would be required to do something similar but the handset manufacturers might be able to create and embed something in the hardware which is turned on by default as a guarantee or fallback.

---ooo---

[7] In the UK all the mobile phone companies put gambling, pornography and similar age sensitive services behind an adult bar by default. The same is true in most of the rest of Europe. The bar can be lifted. Different companies have different ways of allowing the bar to be lifted but in each case it involves the user proving they are over 18.