

Localisation of mobile terminals and personal data protection

M Marcel Pinet

Member of the National Processing and Liberties Commission, France

Whether it concerns proposing the fastest route for you to get home after leaving the office, allowing you to order your dinner at the nearest restaurant, or showing you precisely where to find your child who is late, the so-called « geolocalised » or geo-dependent services are presented as the most powerful “leaven” for the development of mobile communications services. Geographical co-ordinates of base stations, triangulation, GPS, these are all technologies implemented to calculate localisation information; they have been widely presented and commented, so we will not cover them here. On the other hand, we will cover that which is essential, meaning the implications of the development in these services and the consequences on privacy and personal data protection, which will allow us to approach the bases of their regulation.

A reminder: what are we talking about?

We are talking about processing which consists in specifying the geographical position of a terminal which is not switched off, that is to say, on stand-by or in conversation, moving in a network of mobile communications, in order to either present these localisation data to a person looking for the owner of the mobile, or giving these data to a supplier who will use them to offer his services according to the place where the user is at any given moment.

It should be pointed out that in France and in the member countries of the European Union, the legal framework around this problem is not only constituted by the respective national laws, but also by the European Directive n° 95/46 of 24th October, 1995 and the draft proposal for a directive of Parliament and the Council of 12th July, 2000, concerning the processing of data of a personal nature and the protection of privacy in the electronic communications sector. As for other countries around the world, everything obviously depends on local situations, but it is also necessary for a minimum of fundamental principles to be taken into consideration.

I. Geo-localised services - a game for several players

A. The user

He is invited to consume the services offered to him, for direct or indirect remuneration of the chain of providers involved in the supply of the services.

B. The technical provider, namely:

- the operator: he is the owner of the network and the SIM card which is necessary for connecting a mobile to his network; he is master of the localisation information, or at least of the access to this information. The operators equip their networks with localisation functions by using platforms allowing them to calculate their clients' geographical co-ordinates. They may either merely

transmit this information to service providers for direct or indirect remuneration, or themselves propose all, or part, of a range of geo-dependent services.

- the supplier of the localisation technology: he is above all an editor of software which allows people to calculate and valorize the localisation information in order to transmit it to a service platform. He may either merely sell his localisation « solution », or enter into agreements with operators or service providers.

- the « infomediary » who develops a platform implementing localisation techniques with the different national operators, in order to propose the mobile users' geographical co-ordinates to service providers. Their main advantage is the « single counter » function they offer between operators and service providers: in dealing with an « infomediary » the service providers no longer have to worry about establishing legal and technical agreements with each of the operators for the supply of localisation data.

C. The public collectivity

It is responsible for the general interest and particularly for missions of saving human life and property, but also for detecting and repressing crimes and offences. In this respect it becomes a « natural » consumer of information about localising individuals.

II. Geo-localised services - an ambiguous game in many respects

A. On the side of the user

It is understood, that the only player whose role seems well defined is the user. Appealed to in order to consume new services, he is the one requesting ever more efficient services, or at least he is presented as such.

However, the attitude and expectations of users are not without ambiguity. Quite the contrary, the expectations of geo-localised services, potentially intrusive in our privacy (where am I, at what time, what am I doing, and perhaps even with whom if only this « whom » has a mobile switched on, etc.) should be balanced against the legitimate will of the citizens to see their privacy respected.

B. On the side of the technical services providers

All have an interest in the development of services. Nonetheless, one of the guarantees of privacy is the non-dispersion of localisation information and manipulation of the information by the operator himself who would then appear as the person responsible (i.e., the person who answers) for the use which is made of the individuals' localisation data.

This arrangement, which would be relatively more reassuring, is impossible to apply: mobile communications networks and the implementation of geo-localised services are expensive, and the profitability of such investments would imply that a maximum number of the operators' clients should be users of geo-localised services. He should, therefore, offer them a wide range of geo-localised services; in order to do this, he has to establish partnership links with various service providers so that he can offer the widest range of services possible to his clients, in order to

encourage the use of his infrastructures and, consequently, the return on his investments. The operator should proceed in the same manner as an airline company who establishes agreements with tour operators and travel agencies in order to be able to fill its planes.

C. On the side of the collectivity

It is certainly gratifying to note that the existence of localisation platforms is a comforting addition to the panoply of means at the disposal of the services of rescuing and safeguarding of people and property (emergency medical services, police rescue, fire brigade, etc.).

But we also have to note, that the development of localisation platforms is a real « windfall » for the police services, at a time when the mobile 'phone is presenting itself as one of the principal instruments of communications in organised crime. Who called who at such a time at such a scene of operations, did the protagonists meet before and/or after the fact, where are they hiding; without even at the start having the wanted persons' mobile 'phone number, one could identify them, follow them, arrest them and destroy their bases without them necessarily having confessed: the interests as well as the deviations of such surveillance systems are obvious; in the end, the duty of personal data and privacy protection will here oppose police imperatives.

The movement which is forming is therefore that of a circulation, even a sharing, of localisation data between the various intervening parties in the chain of service providers, with the important necessity of an access to the localisation data by the legal authorities. In such a context, where the limits between the roles of the various intervening parties are not only blurred, but also required to evolve in timing with the development of the services, it is the duty of the authorities to lay down clear rules of the game to ensure the protection of personal data and respect of privacy.

III. What legal regulation for localising mobile 'phones?

At a time where the analysts agree that the question of guarantees with regard to the respect of privacy and personal data is one of the major breaks on the development of electronic commerce, legal regulation no longer limits itself to defending the rights of individuals, it also participates in the definition of a specific and protective legal framework indispensable to the development of the services concerned.

At the moment, when a wide and generalised development of these services has not even been achieved, one may attempt an approach based on specific principles which are considered indispensable.

- first of all, nobody must be localised by anyone without his knowledge, except by the emergency and rescue services to safeguard human life and property
- the localisation data must not be stored after the service has been rendered
- any disclosure to a third party must be subject to the person concerned being informed. If this third party is extraneous to the service provided, this disclosure must necessarily be subject to the consent of the person concerned.

However, these principles, which appear so simple, may become redoubtable as soon as one tries to apply them.

The principle of prior information and consent poses the question of its technical implementation; should one conceive the terminals or, in any case, the localisation software equipping these, in order to submit execution of any localisation request to the consent of the owner of the mobile? Should this authorisation be granted case by case, service by service, request by request, or once and for all, naturally with the possibility of the user retracting the agreement?

One can easily agree, that a person whose geographical position I wish to know should be asked to give his agreement to such a localisation. Would I, on the other hand, accept being ceaselessly disturbed by the beep of my mobile asking for my agreement when I am lost driving my car and using a navigation aid service, which to be efficient must localise me every twenty seconds?

In the same line of thought, the operator who calculates a localisation and transmits it to a service provider must immediately delete it: he has only determined the localisation in order to transmit it. The service provider may store it if he has to invoice the client according to either the place or the service to be delivered. Consequently, it is necessary to remember that the operator no longer has the localisation data but that the provider still keeps these. And if the provider is abroad, that poses the question of applicable law and of the effectiveness of people's right concerning processing of a localisation in a place where the national law of the person concerned does not apply.

Moreover, is it desirable that within the framework of certain procedures which come under its constitutional and legal competence, the legal authority could have access to the localisation of people who are suspected of or authors of offences or crimes?

Should we, consequently, envisage a certain duration of storage of these data for this purpose, and if so, what should this duration be?

Should we go as far as admitting that police services could use the localisation platforms to follow, without their knowledge, and in real time, the people suspected of acts constituting crimes or offences?

It is clear that the application of the principles of protection of data and privacy is much more complex than it first appears. For the moment, they are still applied case by case according the realities of services and countries.

Consequently, an international reflection appears indispensable. I hope that our debates here today will contribute to making progress in the establishment of a common platform to face this new challenge of a technology which continues to advance.