Colin Dale, explores ppersonal tracking solutions and their place in the larger counter terrorism and high-level security picture

LOST AND FOUND

©Getty Images

When incidents of terrorism and kidnap meet sophisticated GPS-based personal tracking solutions on smartphones or satellite phones, a diverse range of information is collected remotely by security centres and shared with emergency and other services, including police and intelligence.
The reverse also happens in that users of the solutions (apps) are given information and instructions, based on information gathering by those services that are designed to minimise risk and can involve rescue and evacuation of an area or buildings.

Modern smartphones contain an internal GPS chip allowing them to accurately determine their position when outdoors. When indoors, other methods such as AGPS (Assisted GPS), Wi-Fi access points and cell tower identification provide additional methods of location information.

The Vismo tracking app uses all available locating techniques to accurately track a mobile phone wherever its user takes it. Locations are reported back via the internet to a secure central Vismo monitoring website. In addition, Vismo-patented technology in the app enhances GPS while

extending battery life considerably, something that is particularly useful when the app has to be used for extended periods of time.

More specifically, the patent covers the design behind the algorithms and innovative operations of the app, which optimise location accuracy without incurring the large battery drain that is usually typical of GPS tracking applications.

It's increasingly likely that individuals that are affected by terrorist-led incidents will be equipped with a GPS tracking app, because (many FTSE and Fortune 500 companies – and a number of UN agencies – are resorting to hiring the app as part of their duty of care towards their employees, plus there is a growing uptake of the app by the self-employed and employees in smaller organisations and other individuals that are starting to take personal responsibility for their own safety.

That's no surprise, due to the risks posed by terrorists in formerly safe metropolitan areas and airports in the West, East, Middle East and elsewhere. But also dotted around the globe are computer systems and security centres that provide

previously or is currently happening and gives them instructions as to what to do and the best way to behave to remain safe.

So what happens to any information that's provided by the user? First, the app provides a precise location for them to see where they are. That, along with information given by SMS and/or perhaps spoken by the user, is then put into a third-party mapping solution that is typically used by emergency and other services in the UK and overseas.

This mapping solution provides detail not only at street level but also in some cases individual building level too, helping police, rescue and intelligence services to analyse the situation in real time. Reported information from the app users' SMS messages, spoken messages, photos or videos and from other sources can be useful in helping those services identify who the attackers and any of their accomplices are.

Additional useful information may also be reported via geo-fence and country-change alerts. Geo-fenced areas may be particularly high risk or perhaps safe areas within a generally high-risk country or province. App users (or a third party on their behalf) can define geo-fence areas by drawing them on a map located on a secure monitoring website. The geo-fence can be customised to the desired shape, defining any part of a country, region, city, airport etc. If an app user inadvertently enters a geo-fenced area, security teams are immediately notified and the user is located and guided back into a pre-defined area of safety via email, SMS alerts or by a phone call depending on the specifics of their situation.

Email alerts contain mapping images showing the immediate area, the geo-fenced area and a pin for the phone's current location. Where users change countries while traveling, alerts showing their source and destination country are sent.

If a kidnap situation has been initiated and an app's panic button is activated, a different type of response will be used involving specialist teams including negotiators and rescue personnel. If the phone has been discovered by captors and disposed of, the initial covert recordings and location of the kidnap can provide vital clues that will be fed into shared information among the various services that become involved.

For individuals that are unfortunate enough to get caught up in an extended situation, the app comes into its own. As described, it uses patented technology to improve location finding and extend battery life. Fundamental to its approach is how Vismo utilises the functionality of mobile devices to minimise the use of navigational sensors by placing them into hibernation between pre-determined intervals and using environmental information to locate the handset quickly without a lengthy GPS warm up.

That approach produces a chronological trail

the support that's needed by those unfortunate enough to get caught up in incidents.

When an attack or attempted kidnap occurs, individuals equipped with a GPS tracking app may be the first to report the incident as they will be aware of the need to activate the app and press its associated panic button. As soon as the panic button is pressed, covert audio recordings initiated by the app are then made and transmitted by their phone to the central monitoring server.

If they are able to, individuals can additionally send text messages seeking help or medical attention or more information on their current situation. They are not encouraged to speak into their phone unless it is safe for them to do so; however, users can record a number of covert audio clips, which again will be sent back to the central monitoring server.

If a security centre is the first to know of an incident, its personnel will see at a glance which users of the app are in – or close to – the area or areas involved in the incident and initiate an automated procedure, which firstly sends an SMS to the user. The SMS alerts them to what has happened

©Getty Images

following a user's location point by point on a map and help to guarantee comprehensive and accurate international tracking of the user.

Privacy can be requested for travellers that wish for their location to be identified only when the panic button is pressed, while having their location hidden in normal day-to-day operation. This means that users can now control when they are tracked without having to deactivate and reactivate the app. In the scenario where a terrorist incident has occurred, the likelihood that a user will have the wherewithal to de-activate the privacy mode or press the panic button is unlikely. In this situation, privacy can be remotely de-activated by the incident control room to allow the location of all users to be identified.

In summary, the latest in communications and computing technologies, combined with specialist and commonly used software, enables information coming from, and going to, users' phones – along with other essential information – to be shared across all relevant services, intelligence included, in real time, allowing close collaboration and sharing of resources and effort, nationally, regionally and globally.

Over recent months, and following the increase in terrorist incidents, companies are rolling out Vismo to all travellers not just those travelling in what are deemed to be high-risk areas. This has recently been reinforced with the news from Sir

Bernard Hogan-Howe, the Metropolitan police commissioner, who warned a terrorist incident on UK shores is "highly likely". The current threat level for international terrorism in the UK is severe, meaning an attack is a distinct possibility. There is only one level above severe: critical – which means an attack is expected imminently. The threat level in some other countries is also very high.

The threat level has been at severe since August 2014. It was announced by the then Home Secretary Theresa May as a response to conflict in Iraq and Syria, home to terrorist groups such as ISIS.

Vismo users have been caught up in terrorist and kidnap situations with positive outcomes. For example, the app was involved in the handover by ISIS of the hostage Daniel Rye Ottosen in 2014. Danish photojournalist Ottosen was held by his captors for 13 months until his arranged release in Syria. Members of the team that met him at the handover and led him to safety were in possession of the Vismo app. Situations such as this can rarely be predicted with any certainty and experience demonstrates that they can come completely out of the blue. However, by using a combination of mobile (or satellite) telephony and a specially designed app, and by making optimal use of information shared across the spectrum of support and intelligence agencies, risks can be greatly reduced.

If the phone has been discovered by captors and disposed of, the initial covert recordings and location of the kidnap can provide vital clues

Colin Dale is Business Development Director for Vismo Global Tracking Solutions. For the past 30 years he has worked with mobile and satellite operators including T-Mobile in the International Roaming field. He has a degree in telecommunications from Liverpool University and is currently studying international terrorism at St Andrews University