NOV/DEC 2013

Navigation news

£5.00

The Magazine of the Royal Institute of Navigation

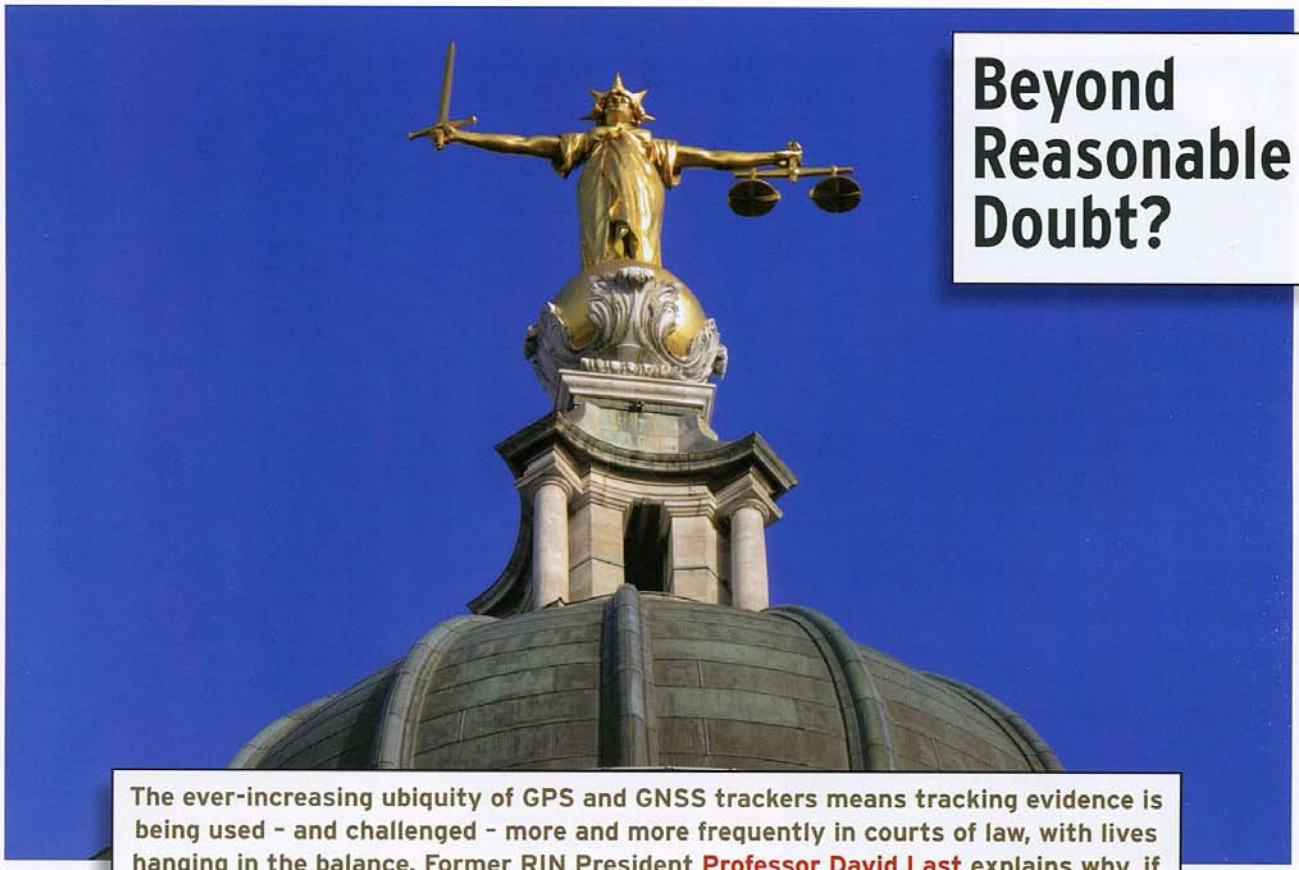
Beyond Reasonable Doubt?

Silva Anniversary
Celebrating the invention of a navigation essential.

Eight Poles
Reaching all of the Earth's polar points.

Because It's There
Going off the beaten track for beauty.

PLUS International News, Navigation Events, RIN News, People, Places and much more...



Beyond Reasonable Doubt?

Picture: istockphoto.com/TonyBaggett

The ever-increasing ubiquity of GPS and GNSS trackers means tracking evidence is being used – and challenged – more and more frequently in courts of law, with lives hanging in the balance. Former RIN President Professor David Last explains why, if it is to be used this way, GPS data must be better understood.

On an August morning in 2011, Rimas Venclovas left his home in Lithuania. He drove across Poland, Germany, the Netherlands, Belgium and France to the port of Dunkirk. He took a ferry to Dover then headed for the home of his former wife… whom he abducted and murdered. Hiding her body in his vehicle, he retraced his path across Europe. Just before dawn in Poland, he turned off a highway, drove into a wood, dug a shallow grave and buried the body, before returning home.

Fig NAV2417.

The jury in this case were shown tracks like those in *Fig NAV2417* which records his whole journey to the UK. Last November, Venclovas was found guilty of murder at the Old Bailey and jailed for life.

GPS tracking evidence like this is compelling and its importance in the legal process is increasing. Trackers are deployed by law enforcement agencies in covert operations. Tracking data is also recorded by many employers, especially logistics companies. They use it as a management tool but also as evidence when they accuse their employees of theft, fraud or malpractice. VOSA (the Vehicle and Operator Services Agency) seize commercial tracking records from trucks as evidence of vehicle offences, including tachograph fraud.

Motor insurance companies have developed telematics products, with units on their customers' vehicles that analyse driving styles, letting the company match premiums to risks. In a collision, these devices log detailed GPS tracks plus the vehicle's accelerations on three axes, which illustrate the event graphically and precisely. They help the insurer identify fraudulent staged 'crash-for-cash' claims.

The Tracks of Your Fears

The criminal fraternity are enthusiastic users of GPS tracking. They target their rivals and their wives (or girlfriends, and often both)! Such tracking evidence has helped secure convictions, notably those of the very criminals who recorded it.

Most GPS records are created by a tracking system: an on board receiver sends its location at intervals to a Tracking Centre.

Fig NAV2414a.

The data travels via the mobile phone network using GPRS (the General Packet Radio Service). The tracker's owner logs on to the Tracking Centre to see the vehicle's location and history. This technology also supports the road user pricing schemes so beloved of European governments.

Fig NAV2414b.

For covert tracking, an owner can send a text message to a device like that in *Fig NAV2414a*, which replies with its location. Alternatively, tracks are recorded by a logger and downloaded after it is recovered *(Fig NAV2414b)*.

By avoiding GPRS radio transmissions, the tiny batteries in these devices can support long-term covert operations.

A Clash of Worldviews

Tracking technologies are impressive to satellite navigation enthusiasts. But when their records become evidence in criminal or civil cases they are exposed to attack in the adversarial realm of the court. Lawyers and navigators view the world differently! Faced with a record of his client's alleged journeys, defence counsel may ask: Who provided this data? How professionally was the tracker installed in the vehicle? What forensic evidence trail was followed? Who could have altered the records? And how accurate are they, especially at crime scenes? Engineers' concerns about the vulnerability of GNSS based on experience of satellite failures, solar storms and radio interference plus intentional jamming and spoofing, will be used to attack the integrity of GPS evidence.

In the Venclovas case, that evidence had been recorded by the satnav in his van. This had a built-in logging mode designed to record its journeys. Users sometimes engage this little-known mode inadvertently - even we experts are barely in control of our own satnavs! I doubt the hapless Mr Venclovas meant to log his every movement as he left Lithuania intent on murder, but log them he did.

So, as in many other cases, there was no professionally-certified GPS installation. The forensic trail started only when the vehicle was seized. Such cases rely on an expert witness to verify the data, show that it is accurate and reliable, explain it to the jury and the court, and respond to hostile cross-examination. The defence will seek out weaknesses in the tracking record and, if these cannot be explained clearly, try to have the evidence excluded from the case.

Objection!

It is right that GPS tracking evidence is challenged in court: GPS is a vulnerable system that can and does fail in various ways. Let us look at some of those challenges; they apply to many applications of GPS, not just court cases.

Defence counsel may cite past satellite failures that have caused large position errors across a region, or losses of service due to solar flares. Can we show there were none at times critical to the case? Happily, vulnerable GPS is monitored intensively. Records of NANUs (Notices Advisory to Navstar Users) and Operations Advisories show the health of the satellite constellation on any date in question. Locally, a network of monitoring stations - some 180 across the British Isles operated by the Ordnance Survey and others - record position fixes at frequent intervals. In the Venclovas case, a British station close to the place of the abduction and a Polish station close to the grave-site confirmed normal and accurate GPS operation.

A tracking record has to be audited with great care. Improbable as it may seem, quite dreadful things are done to GPS tracking evidence! Usually the record is a simple list of the dates and times of a set of position fixes, each a latitude, a longitude, often an altitude and possibly a speed and heading. In a commercial tracking system, this data will have been encoded for transmission to the Tracking Centre and there decoded.

Errors actually detected by auditing in court cases have included: inadvertent transposition of the tenths and the hundredths of seconds of arc in all latitude and longitude readings; excessive truncation of data records to minimise communications costs; data sets in which every location was labelled with the time of the following fix; and confusion over datums. The consequences ranged from position errors of tens of metres to nonsensical tracking evidence with fixes at identical times lying hundreds of metres apart and the ignition of a vehicle being switched on far from where it had previously been switched off! Not all practitioners in the commercial tracking industry meet the professional standards of RIN members!

Reverse Geo-Coding

Even the most competent navigators can fall into traps. Take *'reverse geo-coding'*: a transport manager reviewing the misdeeds of a white van man will want a trail of addresses, not latitudes and longitudes. So, the tracking company's computer will seek the nearest street, or house address, to each position fix. In an armed robbery case in Leeds, a covert GPS logger had been installed on a suspect's vehicle which eye-witnesses confirmed was parked overnight. Evidence from the logger was presented using street names identified by reverse geo-coding. The defence attacked: several fixes were in streets hundreds of metres from where the vehicle had spent the night. Clearly, the tracker was defective and all its evidence should be excluded from the case!

Fig NAV2432.

What has happened? Navigators (unlike lawyers) expect GPS fixes to be scattered around a receiver's location, as in this event (the black dots in *Fig NAV2432*). Reverse geo-coding has sought the nearest road to every fix using a database that represents each road by a single reference point (marked here with a white square). Clearly, many outlying fixes lie closer to the reference points for other streets than to the reference point for Primley Park View where the vehicle was parked. In consequence, reverse geo-coding has increased the scatter from a few tens of metres to hundreds of metres, thereby discrediting the data!

Fig NAV2438.

Imperfect Matches

Another threat to GPS evidence comes from the common practice of map-matching or 'snap-to-road'! Most car satellite navigators take any fix that lies off the road on which the vehicle is travelling and pop it back onto the road. Indeed, most drivers have only ever seen raw GPS data, warts and all, on a rare stretch of brand-new motorway. Map-matching makes satnavs look good; but applied to GPS tracking evidence it can be attacked as gross, undocumented, unauthorised tampering with

forensic data! Although Venclovas' navigator showed a map-matched track on screen, it logged raw data and so recorded off-road excursions accurately.

Evidence obtained serendipitously, as with Venclovas, will come under attack. How can one demonstrate to a jury that it truly records a journey? Sometimes ANPR (Automatic Number Plate Recognition), CCTV, cell-siting or even eye-witness evidence can be overlaid on the GPS tracks, providing firm corroboration. Lacking this, GPS records can be verified in other ways. If they contain altitude readings, these can be compared to the mapped altitude at each location. The Venclovas satellite navigator when driving along roads in Fenland recorded altitudes of some 5-6 metres. The road surface there lies just a couple of metres above sea-level, the GPS receiver perhaps a metre higher. This close agreement lent confidence to the data. And for miles there every fix fell on the carriageway, just 6 metres wide, as *Fig NAV2438* shows. Following the time labels, one can watch the vehicle slow down, turn back, go forward again, then accelerate – just as it had done. When a jury examines GPS evidence of this quality, common sense tells them it's for real.

Multipath - Counsel's Confusion

But not everywhere is as GPS-friendly as the Fenlands, where there are few buildings and 2 metres above sea-level counts as a bit of a mountain! When the accuracy of GPS evidence is challenged, the answer can be surprising. Earlier, in *Fig NAV2432* we saw that some fixes lay almost 100 metres from the centre of the cluster where the vehicle was parked – excessive errors for a suburban location. On visiting the scene, the reason became clear: an 11-storey building immediately across the road from the parking spot, which blocked direct signals from satellites to the south. Another building just behind the vehicle, to the north, reflected these signals; classic urban multipath propagation. Though GPS tracking fixes on an open site may be clustered within a few metres, multipath propagation elsewhere may cause errors of up to 300 metres in the same tracking record. In the mean streets of a city, multipath dominates accuracy!

Fig NAV2440.

Multipath errors are also found in unexpected places. When Venclovas' vehicle passed through Dover Eastern Docks, the tracking record became badly scattered: it jumped forward 50 metres in just one second, then doubled back, then leapt into an office building. The cause: multipath errors from the White Cliffs of Dover *(Fig NAV2440)* which rise almost vertically beside the outbound traffic route, blocking satellite signals from the north and reflecting those from the south.

Navigation professionals expect position fixes to be scattered around a receiver's location. Many laymen – and lawyers - assume that a satellite navigator is right where it says it is; and if you don't move it, that's where it will stay. This misconception can lead to miscarriages of justice.

Fig NAV2341.

Truck Leapfrog

A group of lorry drivers were charged with tachograph fraud and threatened with imprisonment. They would park overnight and sleep in their cabs. But, as illustrated in *Fig NAV2341*, the tracking record (little bulls-eyes) would show a truck jumping randomly between discreet locations, none more than 30 metres from where it was parked. The prosecution claimed the driver had driven his truck and not recorded this on his tachograph. Common sense asked: why would he spend his night shuttling around the parking lot? A GPS expert sees a stationary tracker, with multipath reflections from a large metal-clad warehouse alongside, and latitude and longitude scatter quantised in 10 metre steps to save communications charges. With that explanation finally accepted, no driver was imprisoned.

Thank You, The Da Vinci Code...

Many laymen also assume that GPS works everywhere – perhaps unsurprisingly, given Hollywood's portrayal of GPS as doing precisely that, to the mortification of those in the know. Increasingly, white van men are being charged with theft on the basis of GPS data recorded by their hand-held terminals (the device on which you try to sign your name!) In a recent case, a delivery was signed for deep inside a shop, as confirmed by CCTV there. But the GPS evidence conflicted with this: it showed the signature as being outside in the street. The driver was acquitted.

What had happened? Lacking usable GPS signals inside the shop, the terminal had substituted the last valid fix the driver had taken when scanning the parcel at his van. If GPS evidence is to be used in criminal cases like this, the behaviour of GPS receivers in areas of weak signals must be understood - beyond reasonable doubt.

GPS evidence is not like other digital forensic evidence: as navigation professionals understand, the accuracy, integrity, availability and continuity of GPS depend chiefly on the vagaries of radio signals and the awful things that can happen on their journeys from satellite to receiver. As we have seen, it is essential to detect and avoid the many sources of error that can degrade GPS tracking evidence and to demonstrate that records presented are accurate and reliable. That done, tracking evidence can be compelling.

It can also be deeply impressive. The track in *Fig NAV2443* records the journey of a consignment of cocaine being brought to the UK from Mönchengladbach in Germany. The data is accurate and reliable. Yet it was extracted months after the event by a brilliant computer forensic analyst from an encrypted file in undeclared memory inside a tiny logger.

This GPS device was bundled with the cocaine and buried inside the stuffing of a sofa stacked among other furniture deep inside a removal van. There it managed to pick up satellite signals and gather data. At its best GPS tracking evidence can be quite remarkable. Treated with respect, examined and explained carefully, it will stand up to the most robust interrogation and will often carry the day.

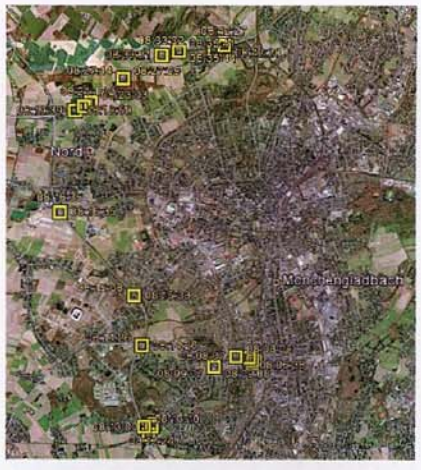


Fig NAV2443.