

# Use of GPS Data as Evidence in Court

***Andrew Dempster (1)***

Australian Centre for Space Engineering Research  
School of Electrical Engineering and Telecommunications  
UNSW Sydney  
+61 2 93856890, a.dempster@unsw.edu.au

## ABSTRACT

There has been a proliferation of the use of GNSS logged data in court as evidence. This paper acts as a short literature survey on the topic, looking particularly at the quality of that data. It does not present new results; rather it identifies areas where research can be developed that results in reliable evidence in court.

**KEYWORDS:** GPS, GNSS, Data reporting, Court evidence.

## 1. INTRODUCTION

Satellite navigation data is increasingly being presented in court to support prosecution and defence of both civil and criminal cases. The range of applications being examined is wide; the range of questions that the Global Navigation Satellite Systems (GNSS) receiver is required to answer is also wider than may appear obvious. Despite this wide-ranging use of GNSS, there are surprisingly few contributions to the research literature on GNSS data used as evidence.

In the early days of the Global Positioning System (GPS), especially when space-based augmentation systems (SBAS) were being developed, the main legal concern regarding GPS was liability for “error”, where the word error could be considered to have a binary value – either an error was made or it was not [1]. GPS and the open Galileo signals were considered unlikely to attract liability but SBAS and the Galileo commercial and safety of life signals were more likely because they were committed to a level of service [2]. It was found that “Space Law treaties cannot solve liability questions about the failure of a GNSS signal” [3]. Efforts by ICAO to develop an international treaty or convention on GNSS liability have not yet borne fruit [4]. The greater exposure of the Galileo commercial and safety of life signals to liability was marketed during system development as an advantage over GPS [5], giving a stick for the Europeans to beat the Americans with, as Selective Availability (SA) was still operating (i.e. Galileo was a civilian system, with guaranteed accuracy, for which they would take responsibility, whereas GPS was a system the US military could arbitrarily degrade to

kilometre level accuracy at any time). This perceived advantage was one reason that SA was turned off six years ahead of schedule [6]. An alternative view to the liability problem is that given the ubiquity of GNSS now, liability claims may start arising when GNSS is not used in some applications [7].

Other issues surrounding the use of GNSS as evidence include privacy [8] [9], the admissibility of GPS surveillance data due to its method of acquisition [8], vulnerabilities [8], and the method of extracting the data from the logging device [10].

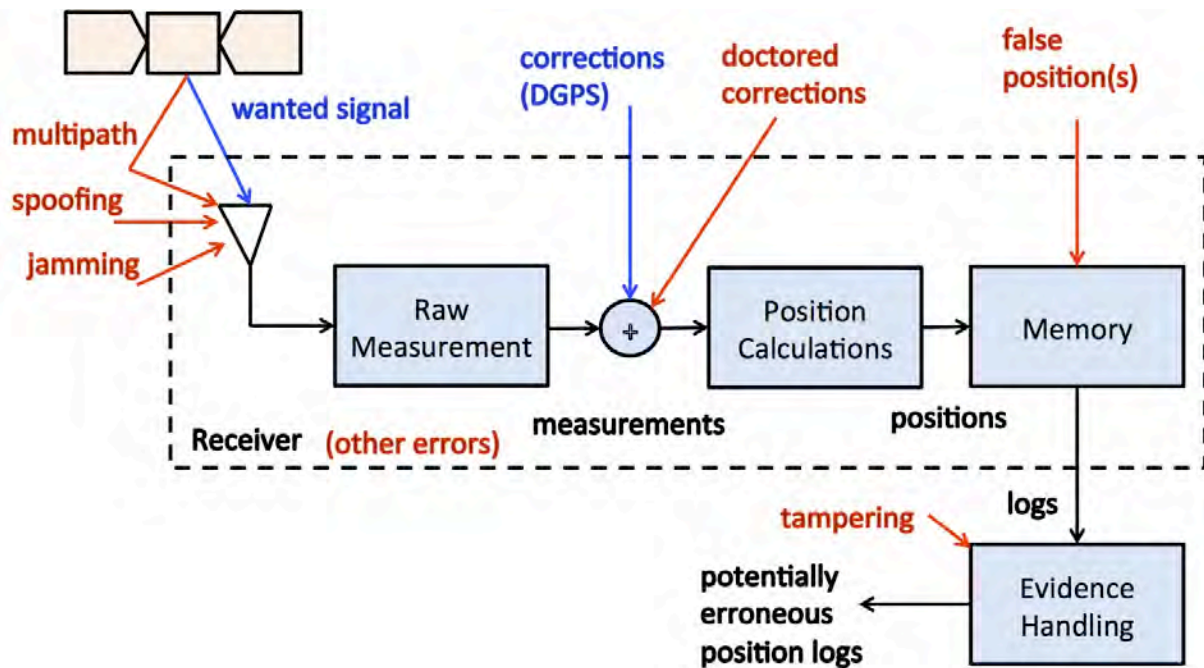
Issues arising from errors in GPS data, or the interpretation thereof, have led to (see the reference list for [9]) police forcing entry in to the wrong home, repossession of the wrong house, and even demolition of the wrong house [11]. A recent study [9] found GNSS data were being used in evidence at a rapidly increasing rate, the range of case classifications was increasing (in 2015, 19 criminal classifications and 11 civil classifications), the weight given to GNSS data in those cases was “high” (8%) or “medium” (54%), and the GNSS evidence was deemed admissible in a significant majority of cases. Given this scenario, the validity of that evidence is of increasing concern.

The main purpose of this paper is to examine the *quality* of the GNSS data presented to a court. This subject has not attracted a large amount of research interest. However, it was examined in [12], which only considered the accuracy of the data and concluded “the prosecution service needs to examine the GPS evidence thoroughly and must present other supporting evidence for GPS evidence to be admissible evidence in court”. This paper argues that (in)accuracy in itself is not grounds for inadmissibility, but the absence of integrity data may be.

## **2. VULNERABILITY OF REPORTED GNSS DATA**

### **2.1 Vulnerabilities**

Figure 1 identifies the various sources of an erroneous position log that may be offered as evidence. There are effects due to the receiver’s environment such as multipath and (not shown directly in Figure 1) attenuation of the wanted signal from the satellite due to blockage by trees or buildings (e.g. trying to track a car in an underground car park, or a tagged offender wearing an ankle bracelet indoors). There are also deliberate attempts to undermine the GNSS receiver’s operation such as jamming (transmitting a radio signal to degrade or destroy the signal to noise ratio received) or spoofing (transmitting a GNSS-like signal telling the receiver it is somewhere else). Incorrect differential GNSS corrections could be sent, and if the calculated positions are transmitted for storage elsewhere, that process could be intercepted and false positions reported. If the logs are stored on-board the receiver or larger integrated device (e.g. smart phone), those entries can be corrupted. There is also the possibility of other errors (bugs) being introduced in the receiver. Once the logs have been collected as evidence, as is the case for all evidence, there is the possibility of tampering.



**Figure 1** Where do erroneous positions come from? In blue are wanted signals, in red potential sources of erroneous output. Note that this is a standard architecture and other variations are possible, such as the memory residing at a remote location. Not shown is another source of error: poor geometry, as would be detectable by a high dilution of precision (DOP)

Examples of occurrences of poor geometry, multipath, weak signals, jamming and spoofing are covered extensively in the literature. A number of researchers have shown how GPS data can be logged legitimately and then modified in situ when data was stored in NMEA format [8], encrypted memory [8], and as geo-tags in smart phones [13]. Also demonstrated was the interception of position and its replacement with false positions when reporting to base [14].

## 2.2 Detection and Mitigation

The question we are considering is how we can make some sort of quality statement about recorded GNSS data, with the aim of understanding how valuable that data is when used as court evidence. Ideally, that information should be useful to an eventual user in determining whether any of the vulnerabilities identified in the previous section have occurred.

The sort of information a receiver can provide that is useful in identifying these threats are:

- Weak signals. Often recorded as low carrier to noise ratio (CNo) or signal-to-noise ratio (SNR), these occur when in blocked environments (e.g. underground car park) or when being jammed. The receiver can measure CNo relatively straightforwardly by examining the correlator output (the correlator function is essential in all GNSS receivers).
- Dilution of precision (DOP). This is a measure of the geometry of the satellites being used for positioning. Poor geometry (high DOP) is likely to result in poor position, regardless of any other factor. The receiver knows the DOP because it knows the time, its own position, and the orbits of the satellites it is using (from almanac data downloaded from the satellites or another source).
- Multipath detection. Many patents record special correlators designed to minimise the effects of multipath. Methods also exist that allow detection of multipath on a single signal. A number of metrics have been developed for this purpose [15] [16].
- Integrity information. Using receiver autonomous integrity monitoring (RAIM) [17],

which is basically a way of using redundant measurements (GNSS or others) to identify and possibly reject poor individual measurements (so multipath could also be detected using this multi-signal approach). This leads to the ability to define protection limits [18], which bound the error of the position estimate to a certain probability – something that would be very useful to have when discussing the validity of evidence.

- Spoofing detection. Various methods can flag if the receiver thinks it is being spoofed, or has transferred from authentic to spoofing signals. Some of these methods are very similar to the multipath detection methods mentioned above [15].

Detection of doctored differential corrections will not be dealt with here.

Detection of tampered logs can be problematic. Depending on the type of log, platform and operating system, some modifications can be made without detection [8] [13].

Detection of evidence that has been tampered with can be done by comparing with data extracted from the receiver a second time.

## 2.2 Data Logging

There is a myriad of data formats in which GNSS data can be recorded (see for instance OpenStreetMaps conversion table at [http://wiki.openstreetmap.org/wiki/List\\_of\\_GPS\\_trace\\_file\\_formats](http://wiki.openstreetmap.org/wiki/List_of_GPS_trace_file_formats)). Similarly, there are many converters between formats such as GPSTabel ([www.gpsbabel.org](http://www.gpsbabel.org)). For general-purpose logging, here we just consider two commonly used formats: NMEA messages and (briefly) GPX (GPS exchange) format.

National Marine Electronics Association (NMEA) standard 0183, more commonly referred to simply as “NMEA”, describes a collection of messages (sometimes referred to as “sentences”) provided by maritime equipment. The GPS sentences begin with “\$GP” and have been adopted by receivers used across a range of application (i.e. not just maritime). The next three characters identify the message type, so a “GGA” (fix information) message begins “GPGGA” and is followed by data. Messages that include position quality information are [19]:

GGA: this message records time, lat, long, fix quality, no. satellites, HDOP, altitude, height of geoid, some DGPS data, and a checksum. On the face of it, this looks encouraging, because this is quite a common message and it explicitly has two quality measures in it: “fix quality”, and HDOP. However, fix quality is simply a single byte identifier stating which type of fix is being reported – GPS, DGPS, PPS, RTK, RTK float, dead-reckoned, manual, or simulated. That is a helpful first step but can only identify the expected accuracy using a particular technique, not the achieved accuracy. Similarly, HDOP, being a geometric measure, can indicate poor accuracy if DOP is high but does not guarantee good accuracy if low.

GSA (satellite status): 3D fix, satellites, PDOP, HDOP, VDOP. By separating HDOP and PDOP, and by reporting whether a 2D or 3D fix was made, horizontal and vertical errors can be somewhat separated.

GSV: (satellites in view): satellites, elevation, azimuth, signal to noise (SNR). The SNR, closely related to the CNo mentioned above, is directly useful in determining whether the position is accurate, and indicates poor performance in partially blocked or jammed situations. From elevation, the likelihood of multipath can also be inferred (low angles tend to suffer

more).

(The above three messages are relatively commonly reported by receivers. The following two are likely to be more useful, but are not provided by all manufacturers, and rarely used by those who do provide them.)

GRS (Range residuals): time (relates to a GGA), residuals for each satellite. From these you can identify if any is affected by multipath or blockage.

GST (Pseudorange noise statistics): time, RMS value of residuals, error ellipse semi-major axis, semi-minor axis, orientation, lat 1 sigma, long 1 sigma, height 1 sigma. This is a good error estimate but doesn't identify which individual measurement is most erroneous, if any is a "rogue".

Some receiver manufacturers produce custom messages which may be useful, such as Garmin's \$PGRME message which directly estimates positional error.

The second data format considered, GPX [20], is commonly used for transferring between platforms GNSS positions (lat/long with time and elevation optional), sometimes in the form of tracks and routes. GPX does not include data types for any sort of quality measure.

Since 2016, Android smartphones have had the ability to log raw GNSS measurements (pseudorange and pseudorange rate, navigation messages, accumulated delta range or carrier, clock) [21]. This allows the user of that data to assess some quality measures at a later stage, such as RAIM and residuals, but still omits others such as SNR.

For systems that are designed with later investigation in mind, there may be an expectation that position quality measures may also be recorded. This is not necessarily the case. For a flight data recorder (the "black box"), for instance, there is no requirement. In fact, "data recorded varies widely, depending upon the age and size of the aircraft" [22]. The ETEP Sentinel records [23]: UTC Time, Status, Latitude, N/S indicator, Longitude, E/W Indicator, Speed over ground, Course over ground, UTC Date, Magnetic variation in degrees, Magnetic variation direction. Many do not record position.

If these high-end recorders do not record quality indicators, it is not that surprising that lower-cost devices do not either.

More recent GNSS-dependent aviation equipment does, however, record integrity. Automatic Dependent Surveillance Broadcast (ADS-B) data includes both accuracy and integrity (in the form of horizontal protection limit) in its messages [24].

Monitoring of maritime vessels using the Automatic Identification System (AIS) does record and report position, and whether RAIM was used but only in terms of whether or not 10m accuracy is guaranteed [25].

## **2.4 Case Studies**

So how would these measures have helped in real cases? As it turns out, quite a lot, and not much. Two case studies are presented here where the author was asked to comment on GNSS evidence in court.

### 2.4.1 Velocity of a vehicle in an accident

The Queen v Shane Anthony Day, 2014/00075246, NSW District Court

This was the case that inspired the current investigation. It included five charges including dangerous driving occasioning death. The expert witness report was to cover examination of data from a GPS receiver installed in a truck that was involved in an accident. The requirement was to explain the data, and “create a sketch using the GPS coordinates to plot the vehicle and the speeds travelled every 10-15m leading up to the collision”.

In this case, the police were trying to establish whether the heavy vehicle was exceeding the speed limit imposed on heavy vehicles on the relevant section of road.

Two sets of data were logged by an on-board GPS-equipped system, and sent to a base where it was stored. One data set was recorded every second, and every minute, 60 of these data points were transmitted. The other set was sent every 20 seconds, or when an event (like turning through a particular angle) occurred. These two sets of data are shown in figures extracted from [26] in Figure 2 and Figure 3. Figure 2 shows the two data sets in green and blue. They are clearly inconsistent. The red plot is an attempt to reconcile them by averaging over 20s – unsuccessfully. No logical relationship between the two sets of data was found, despite the fact they (allegedly?) came from the same receiver.

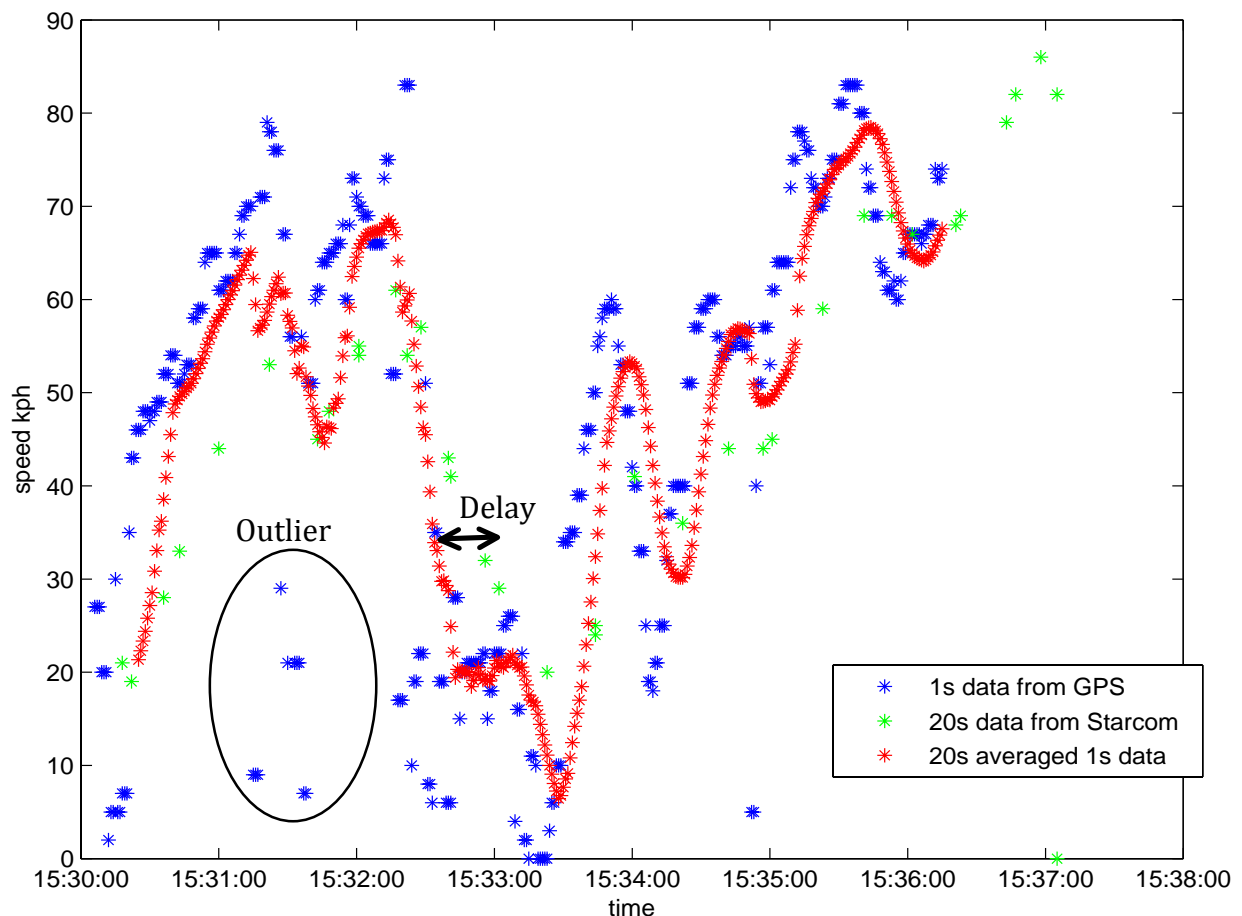


Figure 2 Raw data from the Fleet Effect/ Starcom data in blue and green. Blue data averaged over 20s in red.



The opinion the author put forward in that report was that the 1s data was more reliable than the 20s data, for two reasons: it was more “raw” (according to the manufacturer of the logging system) and it was more internally consistent, i.e. smoother with fewer outliers. These are not strong reasons. Unfortunately, as can be seen in Figure 3, the 1s data ran out well before the accident occurred (at the right of the figure), because a complete minute had not been accumulated for transmission. So in the area of interest, only the less reliable 20s data was available.



**Figure 3 Fleet Effect velocity data overlay: blue (1s) and yellow (20s)**

In a final effort to find more reliable data, speed was calculated [27] using positions and times for sectors of the final section, using 20s position data. This was assumed to be more reliable than 20s speed data, as it places the vehicle nicely within the required lane on the road. These results are shown in Figure 4 and Table 1. Unfortunately, this introduced a third set of data not consistent with either of the previous two (and all from the same receiver!). All three sets indicate that speeding had occurred, but which set to trust? Luckily, the case did not rest on this data, but if it did, this data should have been considered weak.

The problems with this evidence probably fall under the “other errors” category in Figure 1. The internal inconsistency of the data is most likely not due to any external vulnerability, so none of the mitigation methods discussed earlier would have helped add veracity to this evidence.





**Figure 4 Sectors used for velocity calculations.**

Sector	Length (m)	Speed (kph)
S1	358	72
S2	43	78
S3	482	87
S4	150	108
S5	292	96
A1	1148	74
A2	944	89
A3	905	90
A4	442	100
A5	292	96

**Table 1 Speeds for sectors shown in Figure 4**

#### *2.4.1 Location of an individual holding a receiver*

The Queen v Ian Robert Turnbull, 2014/00223920, NSW Supreme Court.

This case included two charges including murder. The report was required to examine data from a Garmin GPS map 60CSx receiver and comment specifically about the accuracy of a set of recorded data.

This is a more straightforward case but it still highlights the problem that even with good data, its quality can only be inferred when it is not recorded explicitly. Plotted on Google Earth, some of the data appears in Figure 5 and Figure 6. Only time, latitude and longitude are provided. The context of the data is: wide, flat country (therefore no multipath or blockage problems), good satellite set (therefore good DOP). On that basis, good accuracy is expected. Further, in Figure 6, it can be seen that there are trees by the side of the road, which may cause



attenuation. However, also in Figure 6, it can be seen that when driving, the reported positions have the vehicle on the correct (left) side of the road, direct evidence of good positioning. It is only with this type of inference that good positioning can be argued in the absence of actual integrity data.



Figure 5 GPS data overlaid on Google Earth: all points

### 3. CONCLUSIONS

#### 3.1 Summary

Many vulnerabilities to GNSS data have been identified. Only some of these can be detected, and when they can be detected, often relevant information is not logged with the data for later analysis. Even in systems such as AIS, only partial integrity information is recorded.



**Figure 6** GPS points overlaid on Google Earth: zoomed to show relationship to the road and to roadside trees.

### 3.2 Future Work

This paper was effectively an investigation to see whether the area of GNSS data as evidence was likely to be a fruitful area of research. It did raise more questions than it answered, so as an exercise it was a success. No doubt there will be many areas of interest that can be further investigated, but future work identified here can be summarised as:

- An investigation into how the legal system would like to see GNSS evidence presented in order to meet its requirements for quality of evidence.
- An investigation into the value of different data to be logged in terms of quality of evidence.
- A comprehensive study of how data logging methods are implemented in standardised and non-standardised logging systems.
- A proposal for a standardised logging method that includes integrity (or other) information that allows confidence in the position to be gauged.
- A proposal for a standardised method to perform and record integrity calculations.

## ACKNOWLEDGEMENTS

Private correspondence with Dr Rod Bryant and Dr Eamonn Glennon has been very useful in the preparation of this paper

## REFERENCES

- [1] Jonathan M Epstein, “Global Positioning System (GPS): Defining the Legal Issues of its expanding Use”, J. Air Law and Commerce, pp243-286, 1995
- [2] Frans von der Dunk “Liability for Global Navigation Satellite Services: A Comparative Analysis of GPS and Galileo”, DigitalCommons@University of Nebraska – Lincoln, 2004
- [3] Juliana Macedo Scavuzzi dos Santos, “The Liability of Global Navigation Satellite System (GNSS) used for Air Navigation in Brazil”, LLM Thesis, Faculty of Law, McGill University, Montreal, 2013
- [4] International Institute for the Unification of Private Law, “Study LXXIX - Third party liability for Global Navigation Satellite System (GNSS) services (2010 - )”, Last Updated: 30 January 2017, <http://www.unidroit.org/studies/civil-liability/393-study-lxxix-third-party-liability-for-global-navigation-satellite-system-gnss-services>, viewed 31 Oct 2017
- [5] Lt Col. Scott W. Beidleman, “GPS vs Galileo: Balancing for Position in Space”, Astropolitics, The International Journal of Space Politics & Policy, Volume 3, 2005 - Issue 2
- [6] Glen Gibbons, “Deselecting Unavailability”, Inside GNSS, June 2010
- [7] Thelen Reid & Priest, “Legal Issues For Companies And Agencies That Use GPS-Based Navigation and Position Technologies: Privacy Issues”, <http://corporate.findlaw.com/litigation-disputes/legal-issues-for-companies-and-agencies-that-use-gps-based.html>, viewed 31 Oct 2017
- [8] Muhammad Usman Iqbal & Samsung Lim, “Legal and ethical Implications of GPS Vulnerabilities”, J International Commercial Law and Technology, vol 3, no 3, pp178-187, 2008
- [9] K J Berman, W B Glisson & L M Glisson, “Investigating the Impact of Global Positioning System Evidence”, 48<sup>th</sup> Hawaii International Conference on System Sciences, pp5234-5243, 2015
- [10] Chad Strawn, “Expanding the Potential for GPS Evidence Acquisition”, Small Scale Digital Device Forensics Journal, vol 3 no 1, pp 1-12, June 2009
- [11] Paul Miller, “GPS coordinates lead demolition crew to destroy wrong house”, endgadget.com, 13 June 2009
- [12] Ishwar Khadka, “The accuracy of location services and the potential impact on the admissibility of GPS based evidence in court cases”, BSc(Hons) thesis, University of Derby, 2015
- [13] Harjinder Singh Lallie & David Benford, “Challenging the Reliability of iPhone Geo-tags”, Int J Forensic Computer Science, no 1, pp59-67, 2011
- [14] Kim Zetter, “Hackers Could Heist Semis by Exploiting This Satellite Flaw”, wired.com, 30 July 2015

- [15] Ledvina, B. M., Bencze, W. J., Galusha, B., & Miller, I, “An in-line anti-spoofing device for legacy civil GPS receivers. Proc ION-ITM, pp. 698-712, October 2001
- [16] Omer Mohsin Mubarak and Andrew G. Dempster, “Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection”, GPS Solutions, DOI 10.1007/s10291-010-0162-z, vol 14 no 4 Sept 2010
- [17] R. Grover Brown, “Receiver Autonomous Integrity Monitoring”, chapter in Global Positioning System: Theory and applications, Bradford W. Parkinson ed., AIAA, 1995
- [18] John E Angus, “Toward Computation of Exact Horizontal Protection Limits for Satellite-Based Navigation Systems”, Navigation, vol 46, no 3, pp217-225, 1999
- [19] Trimble, “NMEA-0183 Messages – Overview” [http://www.trimble.com/oem\\_receiverhelp/v4.44/en/NMEA-0183messages\\_MessageOverview.html](http://www.trimble.com/oem_receiverhelp/v4.44/en/NMEA-0183messages_MessageOverview.html), viewed 3 Nov 2017
- [20] Topografix, “GPX 1.1 Schema Documatation”, undated, <http://www.topografix.com/GPX/1/1/>, viewed 3 Nov 2017
- [21] Android, “Android developer’s API Guides” <https://developer.android.com/guide/topics/sensors/gnss.html>, viewed 2 Nov 2017
- [22] Australian Government: Australian Transport Safety Bureau, “Black Box Flight Recorders”, <https://www.atsb.gov.au/publications/2014/black-box-flight-recorders/>, viewed 3 Nov 2017
- [23] ETEP (Caille Mathieu), personal communication, 22 Sep 2017
- [24] Airservices Australia, “How ADS-B Works”, <http://www.airservicesaustralia.com/projects/ads-b/how-ads-b-works/>, viewed 3 Nov 2017
- [25] International Telecommunication Union, Recommendation ITU-R M.1371-5 (02/2014), “Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band”, 2014
- [26] Andrew Dempster, Expert Witness Report for Police v Shane Day, January 2014
- [27] Andrew Dempster, Expert Witness Report 3 for Police v Shane Day, March 2015
- [28] Andrew Dempster, Expert Witness Report for Police v Ian Turnbull, March 2016