Questions for Providers of Expert Opinion on Logged GNSS Evidence

Andrew G Dempster, *UNSW, Sydney, Australia*
Gary Edmond, *UNSW, Sydney, Australia*
Allison Kealy, *RMIT University, Melbourne, Australia*
Terry Moore, *University of Nottingham, UK*

BIOGRAPHIES

Professor Andrew Dempster is Director of the Australian Centre for Space Engineering Research (ACSER) in the School of Electrical Engineering and Telecommunications at the University of New South Wales (UNSW). He has a BE and MEngSc from UNSW and a PhD from the University of Cambridge in efficient circuits for signal processing arithmetic. He was system engineer and project manager for the first GPS receiver developed in Australia in the late 80s and has been involved in satellite navigation ever since. His current research interests are in satellite navigation receiver design and signal processing, areas where he has six patents, and new location technologies. He is leading the development of space engineering research at ACSER.

Gary Edmond is a law professor in the School of Law at the University of New South Wales, where he directs the Program in Expertise, Evidence and Law. Originally trained in the history and philosophy of science, he subsequently studied law at the University of Sydney and took a PhD in law from the University of Cambridge. An active commentator on expert evidence in Australia, England, the US and Canada, he is a member of the Council of the Australian Academy of Forensic Sciences, a member of Standards Australia's forensic science committee, a member of the editorial board of the Australian Journal of Forensic Sciences, a Fellow of the Royal Society of New South Wales, and served as an international adviser to the Goudge Inquiry into Pediatric Forensic Pathology in Ontario (2007-2008). He is Chair of the Evidence-based forensics initiative.

Allison Kealy is Professor (Geospatial Science) in the School of Science at RMIT University. Allison is currently vice president of the International Association of Geodesy, Commission 4 (Positioning and Applications) and co-chair of the International Federation of Surveying (FIG) Working Group 5.5 on Multi-Sensor Systems. Allison is a technical representative to the Institute of Navigation (US) and is on the Editorial boards of the Journal of Navigation, UK, Journal of Applied Geodesy and the Journal of GPS Solutions. Allison's current research interests include wireless sensor networks, sensor fusion and estimation theory, high precision GNSS, collaborative positioning for intelligent transportation systems and GNSS quality assessment.

Professor Terry Moore is Director of the Nottingham Geospatial Institute (NGI) at the University of Nottingham; where he is the Professor of Satellite Navigation. He has many years of research experience in surveying, positioning and navigation technologies and is a consultant and adviser to European and UK government organisations and industry. He is a Fellow and the President of the Royal Institute of Navigation (RIN) and also a Fellow and a Member of Council of the Institute of Navigation (ION). In 2013 was awarded the RIN Harold Spencer-Jones Gold Medal, and in 2017 the ION Johannes Kepler Award.

ABSTRACT

This is the third in a series of papers with the twin ultimate aims of providing exhaustive guidance for expert witnesses asked for opinion on GNSS data evidence and the development of a standard for GNSS data logging. This paper examines admission of GNSS evidence, then draws on a series of questions noted in an earlier work, and attempts to show how an expert can go about answering those questions to the satisfaction of a court. The paper concludes with a recommendation for a "checklist" that an expert witness can go through in order to establish the level of trust that can be assigned to logged GNSS data.

INTRODUCTION

The use of satellites to generate evidence is on the rise. Data generated by satellites is used in an ever-expanding constellation of legal, quasi-legal and political contexts. Understanding the data produced by satellites as well as interpretations of the data and its limitations are serious issues confronting the increasing array of users. Apart from issues raised through controversies around photographs and their meaning (e.g. whether chemical weapons were produced in Iraq), there is little evidence of serious engagement with the generation of satellite data and its interpretation. As the equipment associated with GNSS becomes more portable and accessible, and derivative evidence more ubiquitous, it seems essential that those producing and presenting this potentially powerful evidence in legal settings should have a clear understanding of both its value and limitations. Data and interpretations (or opinions) based on the data should be reported and presented in ways that are consistent with known abilities.

This article endeavours to direct attention to factors that *may* affect the validity and reliability of evidence generated through GNSS. Our concern is that GNSS-based evidence is generated, interpreted and reported in ways that fairly present its known value. For reasons developed below, we are not confident that conventional rules and safeguards, legal personnel, investigators and jurors are appropriately resourced or generally capable of exploring and evaluating this evidence. In consequence, we recommend that engineers and other experts should pro-actively develop guidelines and standards to ensure the production and presentation of reliable GNSS evidence.

This article begins by introducing the reader to GNSS and some of its potential evidentiary uses. It then explains the importance, for those seeking to adduce, rely upon or present GNSS evidence, of addressing reliability issues; and particularly the recent and authoritative advice from peak scientific organisations on the production and presentation of forensic science evidence. We then turn to consider a range of factors that might impact upon the validity and reliability of GNSS evidence before concluding with a brief discussion.

GNSS might be used as evidence in: border incursions, burglary locations, vehicle velocity, placing people or vehicles at a particular place at a particular time, etc.

A couple of examples are logged speed data in a vehicle accident where speed is thought to have played a part in that accident, corroborating evidence of a witness or defendant who claimed a certain set of movements, placing a defendant at the scene of a crime, and so on. If this data is contested, it comes back to the expert to comment on the degree to which this evidence can be trusted.

ADMISSION AND USE OF GNSS EVIDENCE IN LEGAL PROCEEDINGS

The technical and engineering frameworks that led to the generation of GNSS systems provide an important foundation for the use of GNSS data and interpretations of data as evidence in legal proceedings. These systems place GNSS in a favourable position to address prevailing admissibility standards for expert evidence and enable those responsibly presenting GNSS evidence to explain the data and legitimate interpretations of the data.

In the following sections we will explore issues that may threaten the reliability of data and interpretations generated through GNSS. In this section we introduce a range of influential legal expectations associated with the adduction of expert evidence in some of the most influential adversarial jurisdictions. These rules and procedures are intended to provide some guarantee about the probative value of the evidence and, through reporting obligations and cross-examination, provide basic means of identifying limitations.

It is our general contention that those building and managing GNSS systems – i.e. relevant experts – should develop frameworks and standards that govern how data is generated and interpreted. To assist that goal, in this section we identify three factors that should bear on the way engineers (and others) approach the production of GNSS evidence.[1] They are: (i) the emergence of reliability-based admissibility and procedural rules; (ii) interventions and advice from peak scientific organisations (e.g. the NAS and PCAST); and, relatedly, (iii) the importance of incorporating limitations and uncertainties in the presentation of GNSS data and the interpretation of data to facilitate rational evaluation (and to mitigate resource asymmetries). We begin with admissibility.

[1] We are here concerned with legal proceedings, though recognise that these issues extend to investigations and political uses.

Most adversarial legal systems require those proffering expert opinion evidence in reports or proceedings to satisfy procedural rules and admissibility standards. The most important and influential of these is undoubtedly the *Daubert* standard. In *Daubert v Merrell Dow Pharmaceuticals, Inc.* (1993) the US Supreme Court insisted that to be admissible expert opinion evidence must be 'reliable'.[2] For scientifically-based evidence the Court stipulated that the '[p]roposed testimony must be supported by appropriate validation'.[3] These expectations have since been incorporated into the revised Federal Rules of Evidence and many state counterparts. Not only should expert opinion assist the decision-maker but the Federal Rules now require 'sufficient facts or data', the use of 'reliable principles and methods', and the reliable application of 'the principles and methods to the facts of the case'.[4] In *Daubert*, the Supreme Court provided a list of factors (the *Daubert* criteria) that might be used by trial judges to assist with their gatekeeping responsibilities. These criteria direct attention to: whether the procedure is testable and has been tested; whether the procedure has been published and peer reviewed; the rate of error; the existence of standards; and the extent to which the procedure had attained general acceptance among the relevant specialist communities.

US concern with reliability has been influential on other jurisdictions, particularly common law or adversarial legal systems. The Canadian Supreme Court, most conspicuously, endorsed the concern with reliability, the trial judge's gatekeeping responsibility, and the expectation that issues of reliability should not be abandoned to the trial and the impression of decision-makers.[5] In *R v J-LJ* the Court indicated that the 'admissibility of expert evidence should be scrutinised at the time it is proffered, and not allowed too easy an entry on the basis that all of the frailties could go at the end of the day to weight rather than admissibility.' The Court was anxious that the 'search for truth' in the courtroom should not include 'expert evidence which may "distort the fact-finding process."'[6] New Zealand is another jurisdiction where the *Daubert* criteria have received appellate endorsement – explicitly in the Privy Council – in relation to the admissibility of expert opinion evidence.[7]

Other jurisdictions have embraced reliability or indicia of reliability less directly. In England and Wales, recent amendments to rules of procedure extend judicial attention beyond the expected impartiality of the expert witness to questions of validity, reliability and limitations with the evidence. The *Criminal Procedure Rules* and *Criminal Practice Direction* closely resemble the *Daubert*-inspired admissibility standard proposed by the Law Commission of England and Wales following its review *Expert Evidence in Criminal Proceedings* in 2011.[8] Australian courts also place emphasis on expert impartiality as well as the expectation that expert reports provide sufficient information for trial judges to determine whether opinion evidence satisfies admissibility standards based around the need for 'specialised knowledge'. Australian procedural rules, specifically *Codes of Conduct for Expert Witnesses*, require expert reports to identify limitations, uncertainties, relevant literatures, areas where additional research or testing is required, and even non-trivial controversies.[9] Procedural rules, practice directions and codes of conduct are not admissibility rules per se and non-compliance is likely be considered as an issue for weight.[10]

Other legal systems, including those that were not historically adversarial, may not be formally constrained by admissibility rules or the need for validity and reliability. However, there is a general trend toward reliability that extends beyond the common law world. Nevertheless, to the extent that legal institutions purport to operate in the post-Enlightenment tradition of evidence and proof, all decision-makers – whether lawyers, judges or jurors – must be placed in a position where they are capable of rationally evaluating any expert evidence admitted.

In practice, admissibility and procedural rules, along with calls for judicial gatekeeping, have not led to the exclusion of very much expert opinion evidence. The reluctance to exclude is, somewhat counter-intuitively, most conspicuous in relation to opinion evidence adduced by the state in criminal prosecutions. Most legal systems, including those with explicit reliability standards such

---

[2] Most of the US states followed this lead.
[3] P.590. See also Kumho.
[4] This last phrase bears a striking resemblance to the manner in which PCAST defines validity as applied.
[5] Contrast Australia.
[6] *R v J-LJ* [2000] 2 SCR 600, [35]–[36]. See also R v DD, [2000] 2 SCR 275, Trochym and White Burgess.
[7] See e.g. Lundy v R [2013] NZPC 1, [138].
[8] The government did not adopt the recommendations and so judges undertook to capture these issues in rules of court, rather than admissibility rules.
[9] Though, there is no reliability standard in Australia following Tang, Tuite and IMM.
[10] Serious breaches may lead to discretionary exclusion. See Wood, Chen, and White Burgess.

as the US and Canada, continue to invest trial safeguards with the ability to identify and convey issues with expert opinions and the credibility of experts.[11] *Daubert* exemplifies the prevailing commitment in most adversarial systems.

> Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible [expert] evidence.[12]

Non-adversarial systems tend to be even less restrictive toward the admission of relevant evidence, although there has been an historical preference for court-appointed experts rather than those adduced by parties. In these traditions reliance is placed on the experience of the decision-maker (usually a legally-trained experienced judicial officer) as well as provision for legal representation and scope for witness questioning.

Most of these rules and expectations apply to criminal and civil proceedings. Indeed, the *Daubert* 'revolution' emerged out of civil proceedings in US federal courts. All systems of civil justice maintain rules regulating the production of expert reports, discovery, as well as pre-trial processes and expert testimony (including new procedures such as concurrent evidence). Most of the issues that arise in criminal proceedings have analogies or parallel the way expert opinion evidence is used in civil proceedings. While judges, especially judges hearing cases without a jury, might be willing to admit and consider the weight of evidence that does not strictly comply with admissibility or procedural rules, when endeavouring to evaluate the evidence decision-makers in every type of proceeding should be placed in a position to understand and evaluate (contested) expert evidence.

Unfortunately, opposing parties – and especially the defence in criminal proceedings – are not necessarily in a position to identify and convey issues with technical forms of (expert) evidence. Pressures on budgets, particularly the resources available to criminal defendants, has tended to accentuate problems. Dangers may be acute where, as with GNSS evidence, the underlying systems appear robust or self-evident and issues and limitations may be unfamiliar to investigators (e.g. police) and other non-expert users and audiences. It is with the knowledge that traditional trial safeguards have not worked well, along with the need to place decision-makers in a position to evaluate all of the evidence, that we place emphasis on the importance of identifying and explaining potential issues in the sections that follow.

Secondly, in conjunction with the legal move toward 'reliability', during the last decade a number of independent scientific and technical organisations have intervened to provide advice about legal engagement with forensic science evidence. These interventions, following formal reviews – often in the wake of mistakes (e.g. the mis-identification of Brandon Mayfield) and wrongful convictions (e.g. those emerging out of the DNA-based Innocence Projects) – produced unprecedented criticism of both traditional practices in many areas of forensic science and medicine and placed emphasis on the need not only to validate procedures, but to make sure that applied practices are consistent with validation protocols and standards, and results expressed in ways that incorporate limitations, uncertainty and the risk of error (where known).

The most important of these reviews were undertaken by the U.S. National Academy of Sciences (NAS) published in 2009 and the President's Council of Advisers on Science and Technology (PCAST) published in 2016. The NAS report insisted that:

> Two very important questions should underlie the law's admission of and reliance upon forensic evidence in criminal trials: (1) the extent to which a particular forensic discipline is founded on a reliable scientific methodology that gives it the capacity to accurately analyze evidence and report findings and (2) the extent to which practitioners in a particular forensic discipline rely on human interpretation that could be tainted by error, the threat of bias, or the absence of sound operational procedures and robust performance standards.[13]

The NAS report found that many procedures had not been formally evaluated, standards were often vague, few attempts had been made to measure error and uncertainty, and that some types of expression in routine use were 'scientifically implausible'.[14]

---

[11] Cool crucible.

[12] *Daubert v Merrell Dow Pharmaceuticals Inc* 113 S Ct 2786, 2798 (1993). The formal requirement of 'reliability' and willingness to admit 'shaky' evidence sit uncomfortably together in *Daubert*. Though, we should not forget that *Daubert* was an appeal from a civil case. Consider also *Melendez-Diaz v. Massachusetts*, 129 S. Ct. 2527, 2529, 2531-2 (2009).

[13] NAS report, 9.

[14] This is two decades after Daubert.

Both the NAS and PCAST placed unprecedented emphasis on validation (i.e. 'reliable scientific methodology'), the determination and disclosure of error and limitations, developing empirically-based standards, and appropriate forms of expression, as well as the need to address human factors (especially the threat of cognitive bias) where evidence incorporates human interpretation.

These authoritative scientific organisations also directed attention to the need to study and manage risks posed by cognitive bias. Forensic scientists had traditionally ignored dangers raised by exposure to domain irrelevant information and suggestive procedures. Steeped in research from cognitive science and rigorous methodological designs, particularly from biomedical research (where double-blind clinical trials are routine), independent scientists recommended that forensic scientists determine what information is required for specific analyses and blinding the analyst to gratuitous (or domain-irrelevant) information. Strategies, such as sequential unmasking and diachronic documentation, were presented as alternatives where complete blinding was impractical.[15]

Reviewing progress in the years following the NAS report (between 2009 and 2016), PCAST found that many procedures in routine use were either not foundationally valid or not valid in the way they were routinely applied in casework. Moreover, many results were not reported in empirically-based terms that drew attention to the risk of error, human factors and uncertainties. Relatively few reports provided clear explanations of what was done and the reasoning processes involved.

Finally, attentive scientists were critical of the performance of lawyers, judges and legal institutions. They explained that courts could not be expected, or relied upon, to address 'reliability issues' with expert evidence.

> For a variety of reasons—including the rules governing the admissibility of forensic evidence, the applicable standards governing appellate review of trial court decisions, the limitations of the adversary process, and the common lack of scientific expertise among judges and lawyers who must try to comprehend and evaluate forensic evidence—the legal system is ill-equipped to correct the problems of the forensic science community. In short, judicial review, by itself, is not the answer.[16]

PCAST went further recommending that the US federal government should not adduce expert evidence in criminal proceedings unless the underlying procedure was both foundationally valid and valid in the way it was applied and the results reported.

To the extent that GNSS data is entering legal proceedings as evidence in its own right, or to ground expert interpretations, in the wake of interventions by the NAS and other peak scientific organisations, it seems essential that proponents attend to these authoritative recommendations and advice. Unlike many traditional forensic sciences developed in decades before the reliability revolution and the NAS report (e.g. latent fingerprint, handwriting and bitemark comparison), those working with GNSS are relatively well positioned to answer questions about validity and reliability. Moreover, engineers are, at least in principle, capable of managing cognitive issues. It would seem incumbent upon those seeking to adduce or present GNSS-based evidence to ensure that its strengths and potential frailties are disclosed (at least in reports), and that decision-makers are not misled by the evidence or the expectation that non-trivial frailties will be identified by the defence (or opposing parties).

Thirdly, recourse GNSS raises real risks that non-experts and others will be inclined to rely on naïve or impressionistic approaches to the evidence without insight into the range of potential vulnerabilities and limitations. There is also a danger that proponents, whether experts or others (such as investigators), will advance exaggerated or asymmetrical interpretations in the naive belief of accuracy, or the expectation that limitations will be identified by legal opponents and understood by decision-makers. In line with our commitment to presenting expert evidence in ways that embody its known value (and this includes limitations), and sensitive to the frailties of the *legal* reliability revolution and trial safeguards *in practice*, what follows is a discussion of factors that may individually or in combination threaten GNSS data and conclusions generated from them. These are the sorts of issues that should be considered, even if only to be dismissed, in cases where GNSS evidence is contested or perhaps should be questioned.

We accept that GNSS evidence is likely to satisfy most admissibility rules and procedural requirements. Nevertheless, those producing and proffering opinions should be endeavouring to provide decision-makers with the means of evaluating their evidence,

[15] This may be practically difficult in one-to-one dealings with investigating police.
[16] NAS report, 53.

especially derivative opinions. Those producing GNSS evidence should explain their reasoning processes and pro-actively identify limitations, uncertainties and present interpretations in terms that are epistemologically appropriate.

ISSUES FOR USERS

This section draws attention to a number of issues that individually or in combination may influence the data and/or interpretations of data generated through GNSS. While not every issue will arise in every case, these sorts of issues should be systematically considered by those producing and relying upon GNSS evidence.

Figure 1 provides an indication of some of the areas of vulnerability in GNSS systems.

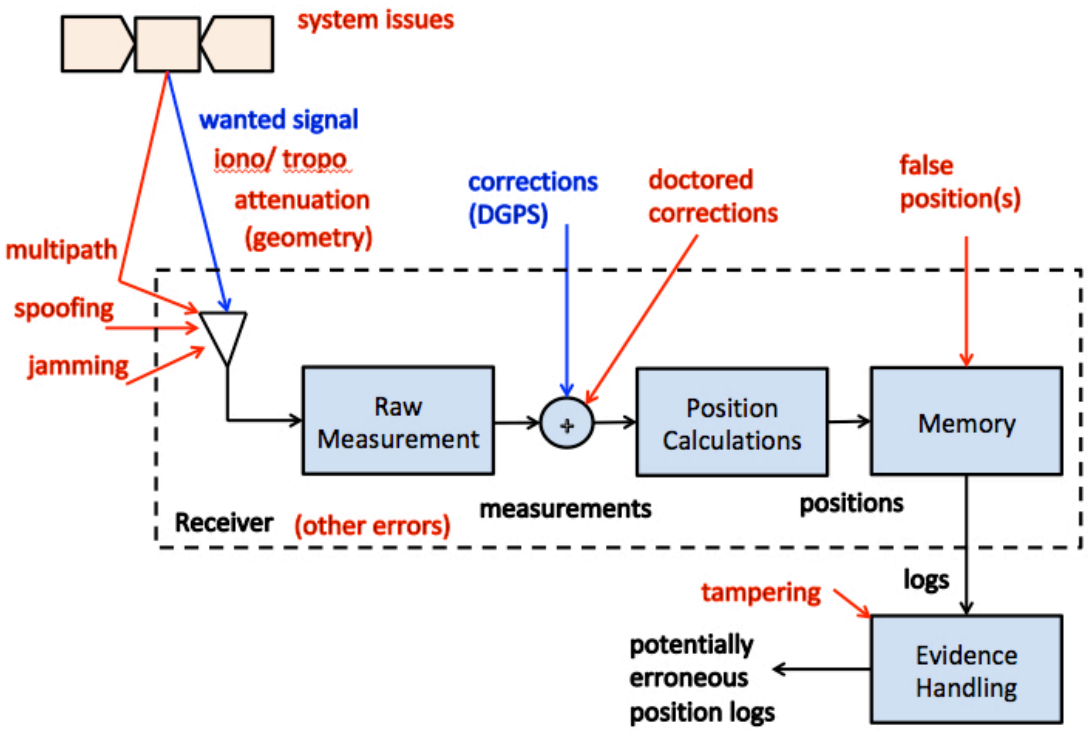

Figure 1: Overview of a GNSS data reporting system, with potential problem areas highlighted in red.

A. System accuracy and integrity

When logged data from a GNSS receiver is used in court as evidence, the positioning system in its entirety is effectively being asked a question, and an expert commenting on only the data obtained from a receiver is asked a different question. For instance, in a case where a person in possession of, or proximity to, a receiver needs to be located at a particular time, the positioning system may be asked "where was that person?" whereas the expert may be asked "how much trust can be put in the position recorded by the receiver at that time?" The question of trust runs right to the core of describing the performance of the positioning system typically expressed for most applications in terms of metrics that describe the accuracy, reliability and integrity of the position computed or derived from the signal measurements between the receiver and the satellites. The accuracy question can be broken down into separate questions, including trust in the positioning system.

Typically, the receivers under discussion are not designed to provide the information required immediately to answer many of the questions posed by investigators and lawyers and the reliance on proxies, where available, has become the default mechanism for

composing a response by an expert witness. There are however, a number of approaches that can be applied before and/or after logging of the data to answer one or more of these at once. These are:

1 Receiver based techniques
2 Integrity
3 Encryption
4 External monitors
5 Authentication by corroboration

The purpose of this paper is to consider how each question might be addressed in order for a court to have confidence in the logged GNSS data presented as evidence.

Q1 Was the GNSS System operating properly?

After the fact, it is possible to check if there were significant problems with a GNSS by referring to the advisory notices published for that system. For GPS, these are called Notice Advisories to NAVSTAR Users (NANUs) and times and dates can be searched at the US Navigation Center (www.navcen.uscg.gov/?pageName=selectNanuByNumber). For Galileo, they are called Notice Advisories to Galileo Users (NAGUs), (see www.gsc-europa.eu/system-status/user-notifications). Other systems provide similar services.

Included in the navigation data are flags indicating individual satellite health, which the receive can monitor. These health bits are not updated very rapidly, so it may occur that a satellite has begun to behave erratically without the health bit yet warning users. At any given time, the status of individual GPS satellites can be checked at the US Navigation Center (www.navcen.uscg.gov/?Do=constellationStatus).

This possibility of a health bit not yet being set when it is needed was the motivation behind the development of Space-Based Augmentation Systems (SBAS) to provide integrity for aviation users, i.e. a ground based network of monitors would swiftly detect a satellite failure and report that failure via satellite using the same L1 carrier frequency as GPS L1 to the receiver, which could then eliminate that satellite from its position calculations. Techniques for doing this task in the receiver, Receiver Autonomous Integrity Monitoring (RAIM), were also developed, and can be used to detect other problems, as we will see.

Q2 Was the ionosphere/troposphere behaving itself? Was position affected?

Most jurisdictions have networks of stationary GNSS receivers that are used for geodetic and infrastructural purposes. In Australia, for instance, Geoscience Australia operates the Australian Regional GPS Network (ARGN). By consulting data from these networks, ionospheric (and to some extent tropospheric) disturbances to individual satellite measurements (pseudoranges) can be observed if present.

The effect on the positioning of an individual pseudorange is discussed under Q6 so the supplementary "was positioning affected?" question is omitted from Q3, Q4.

Q3 Was the receiver affected by multipath?

In the absence of any information coming from the receiver, the expert can talk in general terms about whether the receiver was in an environment where multipath is likely. In open farmland, for instance, multipath is highly unlikely; in a high-rise urban environment, multipath (and blockage) is highly likely, with subsequent likely degradation of position. At any given instant, however, it is not possible to speculate as to whether a given measurement will suffer multipath error, and whether that error would be positive (delay) or negative (advance), because in-phase and anti-phase short-delay multipaths cause each of those cases respectively. Long-delay multipath can cause severe delays in the case where the multipath power exceeds the power in the line-of-sight signal and effectively the receiver measures the multipath-affected path as the range.

A GNSS receiver has a number of methods whereby multipath can be detected, and the affected pseudoranges excluded, some of which have been identified by the authors (e.g. [3] detection, [4] exclusion).

Q4 Were any signals attenuated?

This sort of data is often recorded by a receiver. For instance the relatively common NMEA "GSV" sentence includes signal to noise ratio (SNR) data for satellites used in a fix. This is not automatically logged, but can identify individual satellites that may be attenuated. It is relatively easy (i.e. there is very little computational penalty) for a receiver to keep track of the signal levels and report them.

Q5 Was the receiver jammed or spoofed?

Although these two things look similar to an outside malign actor, the receiver effects are quite different. Whereas a jammer, if deliberate, aims to disable the receiver, the spoofer aims to fool it into recording a false position. Unintentional jamming is also possible.

One symptom in a jamming event is decreased SNR, so the same data can be used to identify it as is used for Q4. Other detection methods include monitoring signal levels at different points in the receiver (GNSS signals sit below the noise so the signal levels usually stay very constant). In the jamming case, all satellites will be affected (this may also occur in the attenuation case if the sky is blocked in most directions by the same heavy attenuator – trees, concrete etc).

Detecting spoofing is quite different as the spoofing signal looks "real" to the receiver. In some circumstances, multipath metrics can be used to detect spoofing (e.g. [5]), but there are many methods including looking at where the signals come from, monitoring the incoming signal power, watching for jumps in measurements and/or position, and signal authentication. Generally these can be implemented within the receiver.

In general, the detection of jamming or spoofing is not reported by receivers.

If the expert witness simply has the final positional data to work with, a jammed receiver will start to behave erratically, with large random errors, whereas a spoofed receiver will be "erratic" in the sense that the receiver output looks good, but it reports a platform moving in a way that may not be possible, such as a boat travelling over land [6].

Q6 Was there good Geometry?

This is relatively straightforward to determine. Calculation of Dilution of Precision (DOP) can be achieved by the receiver, or an external observer, as long as the satellites used to position are known. Using the almanac (orbit models), the location of each satellite can be determined and DOP calculated. DOP represents a factor by which the pseudorange error is multiplied to given an estimate of position error. It can be used in advance, to predict the accuracy, or afterwards.

Knowledge of the receiver environment can also be used by the expert to predict the effect of DOP. For instance, in an urban canyon, blockage of low satellites can be expected, leading to an expectation of higher error.

Q7 Were the calculations performed correctly?

This is the problem with the data in the motivating case of [1]. It is very difficult to establish from receiver data alone. Corroborating evidence such as that identified in [2] will almost always be required.

Answering this question is also the only real reason to perform receiver "calibration", i.e. where a receiver used by authorities in a case is taken to a known location to check position, both before and after being used to record location evidence [7].

Q8 Were the data recorded/ communicated/ logged correctly?

This is difficult for an expert to separate from Q7 so the remedies are similar.

Q9 Was Accuracy Indicated?

This is the question of most interest to the authors, in that a receiver does have the ability to indicate the quality of its position, but often doesn't. Often, an accuracy estimate is simply a reflection of the DOP, and possibly the signal strength, or CN0, both discussed above. More useful is an estimate of *integrity*. If GNSS data loggers recorded an integrity indication as a matter of course, many of the expert's problems would be mitigated.

An integrity measure that would be useful in this case is the *protection level*. The receiver can calculate that there is an x% chance that the error in the position just calculated is y meters, where y is the protection level and x is the integrity risk (which may vary for different applications).

A longer discussion below covers how integrity can be used to answer some of the other questions, or at least make them unnecessary to ask.

Q10 Were other sensors or data used to form the position solution?

The answer to this would need to be on a case-by-case basis, depending on the extra information used. Various "correction" data can be provided: differential, real-time kinematic, precise point positioning. Ideally the receiver should report if such data were used and there may be scope for checking that data, depending on the system.

If the extra input comes from, say, an inertial sensor (accelerometer, gyro) then the integration algorithm will determine accuracy and is likely to be unavailable to the expert.

Q11 Were the data extracted and handled properly?

The procedures here are very similar to standard digital forensics, described briefly in [2]. There are some requirements for procedures that are peculiar to the GNSS case (unpublished but still public domain in the form of courses), such as not turning the receiver on after seizure until it is secure. The receiver itself can of course record a position in a non-secure area if this procedure is not followed, undermining its own evidence.

B. Related issues

Answering questions: the receiver

This section is really about what a GNSS data logger could provide at its output to answer the questions above, i.e. what sort of data reporting could be written into a standard to maximise the confidence in that data when used as evidence, i.e. metadata.

The receiver's ability to detect system failures is slow (unless detectable by RAIM). Ionospheric disturbance is readily detectable for individual satellites using RAIM, and as a systematic problem if the position residuals are high. A number of receiver-based metrics have been developed to detect multipath (e.g. [3][4]). Signal-to-noise ratios that indicate attenuation are easy to extract from the signal tracking loops and are often already reported [1]. Jamming and spoofing can be detected by the receiver (e.g. [5]). Geometry is also readily calculated by the receiver. A receiver reporting on its own calculation performance and recording is basically asking a user to "trust me" unless some sort of encoding is used to protect the data. The receiver can calculate integrity. It may or may not know if other sensors have been used, combined with its output (this configuration is known as "loosely coupled"). And it can't report on the digital forensics used to provide evidence from its data.

Answering multiple questions

The previous section identified how each individual question can be addressed separately. There are, however, several ways that multiple questions can be dealt with at once.

Authentication

The term "authentication" in the GNSS world has traditionally been applied only to the signals, to detect whether spoofing is present. Here, it is used more broadly, to encompass things like corroboration. So if a witness places the entity whose location is tracked at a particular location, and the GNSS log agrees, there is corroboration to a degree (it doesn't clearly answer the accuracy

question, for instance). Internal and external corroboration is described in [2], where position data is internally very consistent (it indicates driving on the correct side of the road when two directions are compared) and externally consistent (the points lie on a road in e.g. Google Earth). When a receiver passes with high accuracy the calibration test mentioned in the Q7 discussion above, then there is also good confidence of receiver accuracy around that time.

In all of these cases, if accurate positioning has been observed, then it may be possible that all questions except Q9 are in fact dealt with (and Q9 does not need to be). This sort of statement must however be treated with care – a receiver positioning accurately in a field may be affected a short time later if under a tree or near a large reflector. The fact the receiver shows a well-behaved position in a garage may actually mean that it has been spoofed to say it is there or jammed and is simply holding its previous position.

Integrity

If integrity calculations are performed in the receiver (answering "yes" to Q9), and a safe protection level has been produced, then it is highly likely that questions 1-4 are also dealt with. If there is a problem calculating and recording position (Q7, 8) there is also likely to be a problem in the integrity calculation so it cannot be used to detect those faults. It may help if external data/ sensors are used but the integrity must refer to the *integrated* solution.

The question of integrity requires a broader discussion of the requirement for statistical techiques that offer a more robust and defensible approach to discussing the validity of the coordinates or velocities provided by the receiver. For example, in the case of the integrated solution discussed above, the estimation process used to compute the position will provide statistical quantities that support better detection of biases or anomalous behaviour, thereby answering several of the questions listed in this paper.

C. Summary

Table 1 serves as a summary of this section and can be considered to be the main output of this paper. The table itself is starting to look like a checklist that could be provided to expert witnesses, and the column referring to receiver capabilities is the basis for developing the standard for GNSS data logging.

Work is continuing and further questions are being raised, so this is unlikely to be the final paper in this series. Admissibility, guidance to the court (as opposed to the expert), and some more work on logged data types are just a few areas that are requiring extra effort.

Question	Source of Answer	Authenticated by Other "Witness"?	Receiver-Based Detection?	Integrity helps?
GNSS System OK?	GNSS NANU	Y	Y (slow)	Y
Iono/ Tropo OK?	Networks	Y	Y?	Y
Multipath?	Rx	Y	Y	Y
Attenuation?	Rx	Y	Y	Y
Jam/ spoof?	Rx +	Y	Y	?
Geometry OK?	Rx, post-processing	Y	Y	Y
Calcs OK?	Hard	Y	Y?	N
Recorded OK?	Hard	Y	Y?	N
Accuracy indicated?	Rx	?	Y	Y
Other inputs used?	Hard	Y	Y?	Y?
Extracted OK?	Digital forensics	Y	N	N

Table 1 The eleven questions for the expert witness and how they can be answered

DISCUSSION: ISSUES AND INTERPRETATION

Use of the data for other – interpretive – purposes should attend to potential threats to the data as well as the validity of the procedures. If, for example, the data are being used not to locate some device, but a person then the relation between a device and a person should be considered. Similarly, if the question is the movement of a person or the velocity of a vehicle is in question, then both the data and the methods of calculation should be disclosed and explained – along with any limitations.

Where possible, those engaged with the data and any interpretation should search for forms of corroboration. These might be supported by independent witness testimony, speed monitoring devices in vehicles, or ground truthing. Experience suggests that in some cases, and here calculating velocity in a good example, different types of evidence may produce significantly inconsistent results. In some cases the evidence may be very powerful, placing a device and by implication a particular person in a specific location. In others, the significance may be less clear and any meaning open to contestation.

CONCLUSION

Finally, we agree that GNSS evidence should be sensitive to the kinds of issues identified by peak scientific organisations (for the forensic sciences). We also support the expectation that those proffering GNSS evidence should be both demonstrably expert and impartial. We are endeavouring to assist GNSS experts to produce their own standards and protocols rather than rely on what courts might, somewhat arbitrarily, suggest or allow. When it comes to technical forms of evidence courts should be looking to disinterested experts, such as engineers (rather than lawyers), to develop frameworks that assist in the production of reliable evidence and encourage the disclosure of potential problems and limitations. It is only when such evidence is presented 'warts and all' that non-experts – whether lawyers, judges or jurors – will be in a position to evaluate GNSS evidence and use to assist with socially important issues around guilt and liability.

REFERENCES

[1] Andrew Dempster, "Use of GPS Data as Evidence in Court", Proc IGNSS 2018, Sydney, 7-9 Feb 2018

[2] Andrew Dempster, "GNSS Data as Court Evidence: Lessons from Remote Sensing", Proc ION-GNSS+ 2018, Miami, 26-28 Sep 2018

[3] 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, published online 18 February 2010, vol 14 no 4 Sept 2010

[4] Mubarak, O.M., and Dempster, A.G., "Exclusion of multipath-affected satellites using Early Late Phase" Journal of GPS, Volume 9, No. 2, 2010, pp145-155

[5] Chao Sun, Joon Wayn Cheong, Andrew G. Dempster, Laure Demicheli, Ediz Cetin, Hongbo Zhao, Wenquan Feng, "Moving variance-based signal quality monitoring method for spoofing Detection", GPS Solutions , 2018, vol 22 no 83, doi:10.1007/s10291-018-0745-7

[6] Mark L. Psiaki and Todd E. Humphreys, "Protecting GPS From Spoofers Is Critical to the Future of Navigation", IEEE Spectrum, 29 Jul 2016

[7] Florida Fish and Wildlife Conservation Commission Division of Law Enforcement GPS Verification Form, undated

References should be numbered consecutively in the text with numbers in brackets, and appear at the end of the paper in the format shown below:

1. Higgins, M. and Harrell, D. M., "Integrated Navigation for Deep Ocean Positioning," *NAVIGATION*, Vol. 35, No. 1, Spring 1988, pp. 7-9.
2. Asari, K., Saito, M., and Amitani, H., "SSR Assist for Smartphones with PPP-RTK Processing," *Proceedings of 30th International Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017), Portland, OR, September 2017,* pp. 130-138.