Mr Angus M. Marshall – Written evidence (FRS0019)

1. My Lords, I am an academic and a practitioner in the field of digital forensics. As an independent practitioner, with 17 years of experience, I have dealt with prosecution and defence, civil and criminal, cases throughout the UK. I am currently employed as a Lecturer in CyberSecurity at the University of York and continue to provide specialist digital forensic services through my own micro-business, n-gate ltd. I am registered as an expert advisor with the National Crime Agency and am regularly consulted by UK law enforcement agencies for assistance with complex digital evidence. I have been a member of the Forensic Science Regulator’s working group on digital evidence and am currently a member of the BSI IST/33 Information Security committee on whose behalf I act as UK Principal Expert on Digital Evidence to the ISO/IEC JTC1 SC27 information security committee. In that capacity, I acted as editor for, and led the development of, two international standards for digital investigations in conjunction with national experts from around the world. I have carried out funded research in cybercrime, digital forensics and computing, and have designed, delivered and examined educational programmes at all levels from BSc to PhD.

2. In this evidence, I will restrict myself to dealing with the following questions raised in the Committee’s call for evidence: 3, 4, 5, 6, 8, 9, 12, 13, 14, 15, 16, 17, and, given my area of knowledge and experience, will tend to concentrate on answering those questions in relation to digital evidence in particular.

Responses to Questions

Scientific Evidence Base

3. Broadly speaking, modern forensic science can be split into two distinct categories. Those whose basis lies in fundamental science such as chemistry, biology or physics (the "traditional") and whose methods can be traced back to principles which underpin that science, and those whose basis lies in reverse-engineering.

4. Those disciplines (the "traditional" group) which rely on the principles of "basic" science can, on the whole, be considered sound as they have a considerably body of peer-reviewed evidence for the methods they use. Few, if any, of the methods are unique to the field of forensic science but rather are applications of well understood and tested methods to specific problems in a manner which satisfies the rules of evidence. They also benefit from the fact that the Universe’s laws seem to be quite stable so results do not vary from day to day.

5. Digital forensics is, by far, the most common area where reverse-engineering is required in order to derive evidence from a device. Manufacturers and service providers do not disclose full data about how features of their products are implemented and, in the interests of protecting privacy, take reasonable steps to make data hard to retrieve by anyone other than the genuinely authorised user. As a result, anyone wishing to develop a technique to deal with a new device, data source or data format, may first have to spend considerably time trying to "get inside the head" of the creator.
and make assumptions about implementation based on their own experience and knowledge. Although their efforts may be successful for the situation they are dealing with, there is often little time or resource available to allow for an extension to the more general case and to show suitability for general applicability.

6. There is also a certain mindset exhibited in some organisations that "we mustn't let the criminals know how we're catching them" which leads to a prohibition on publication and, to some extent, wider sharing of information which would allow peer review of new methods and further development more rapidly. Added to that, the commercial tool providers unwillingness to disclose information about their own development and testing methods means that the evidence base for the correctness of many digital methods is extremely weak or non-existent. This does not mean that the methods are necessarily wrong, but that the evidence of their correctness is not available.

**Understanding and use of Forensic Science in the Criminal Justice System**

7. As a specialist practitioner, not dealing with volume casework, most of my role requires the presentation of complex or unusual evidence to non-specialists. Generally, I find that most of the police officers and legal profession have a reasonable understanding of how to use digital devices of various types in a business context, but that very few admit to anything other than a very rudimentary understanding of topics such as Internet communications, encryption, cloud services or mobile device apps. Given that these are now extremely common because of the pervasiveness of smart phones, tablets etc., it creates a need for basic principles to be explained in simple terms before the actual evidence in any case can be subjected to any form of analysis.

8. Furthermore, the perception of these professionals is that a judge or juror's understanding of the technical issues is likely to be considerably lower than their own and that, as a result, further simplification of the technical issues is required. I am not entirely convinced by this argument as I am aware that the general population probably spends more time using some of these services than those who instruct me and interact with me professionally. However, I understand their arguments and find it concerning that there appears to be neither opportunity nor incentive for them to enhance their existing professional skills with some deeper technical knowledge of what has become an essential part of daily life and, as a result, a factor in many cases brought to court.

9. In addition, I find that prosecutors, in particular, do not seem to have time to properly read my reports, or to consult with me in order to fully understand the evidence I have presented. Indeed it has been the case that during the presentation of evidence in chief, I have had to disagree with and correct a member of counsel who has completely misunderstood my evidence because his understanding of the technical issues was based on incorrect assumptions

---

and personal experience of a completely different, but superficially similar, system.

10. There is, I therefore suggest, a need for greater interchange of information between the investigators, legal professionals and the scientists. This should be a three-way exchange so that each may understand the new issues, constraints, requirements, potential offerings and experience of the others instead of relying on "on the job" ad-hoc self-education through the immediate needs of a particular case.

Standards and Regulation

11. In their recent paper\(^2\), McCartney and Amoaka have noted that "Accreditation is not only inconsistent but may be superficial", while Marshall & Paige\(^3\) discuss the concepts of validation and verification and describe how the FSR's implementation of the standards has drifted away from the original intention. This has led to a situation where it is possible for a forensic science method to be accredited without being shown to be technically correct. The guidance documents, issued by the FSR and others, move the focus from showing that methods are correct and then selecting them, based on customer requirements, to one of meeting customer expectations and showing that methods meet those. Given that very few, if any, customers for forensic science services express their requirements in technical terms, usually stating only an evidential requirement, this results in a situation where methods can be accredited without any assessment of their technical fitness being carried out. It appears that the FSR's regime may, as a result, be lending a veneer of respectability to "science" which has not necessarily been properly shown to be fit for purpose.

12. This situation has, to a large extent, been created by the FSR's reliance on experience in the "traditional" sciences to develop methods for the "reverse-engineering" group. Neither post-holder has, as far as I know, examined closely how the ISO 17025 standard is intended to work for non-forensic disciplines and how the "reverse-engineering" disciplines may lack the necessary base of evidence for the standard to be applied to them. (see also paragraphs 3-6, above).

13. There is also concern about the current UKAS accreditation regime. Leaving aside the cost issues, although costs of £10000 to £20000 for an organisation which has an annual turnover of below £100000 is not an insignificant burden, there is concern about the assessors themselves. In the "traditional" sciences, assessment is usually carried out by a team which includes scientists who are experience in the methods which are under assessment, and also in the related science. In the reverse-engineering group, however, because a considerable amount of work is undertaken by re-skilled police officers, or civilian practitioners with highly vocational qualifications, and little experience of anything other than digital forensics work, there seems to be an absence


\(^3\) Marshall, AM & Paige, R, "Requirements in digital forensic methods definition: observations from a UK", Study, Digital Investigation 2018 (2nd draft submitted and in review)
of demonstration of understanding of fundamental principles amongst the assessor pool. As a result, some bizarre recommendations are being made.

14. For example, one organisation has been told that it should include plans to protect hard drives from the influence of solar flares during examination, another that it has to revalidate methods if a computer is moved from one room to another and another that network cables must be tested every month to show that they are working correctly. Even to a casual observer, these are ridiculous recommendations. We do not live in a world where hard drives are routinely damaged by solar activity, where computers change their behaviours because of movement from one place to another or network cables start to introduce hidden and undetectable data errors because they are ageing. These recommendations have appeared because of an undue emphasis on risk management without an understanding of what constitutes a real risk in digital evidence processing, because the basic requirements and constraints have not been properly established\(^4\).

15. We are, therefore, in a situation where a regulator exists and is seeking powers to enforce a regulatory regime which is itself potentially not fit for purpose. These powers should not be granted until a proper review of the problems with the existing regulatory regime has been carried out and those problems solved. It is not the case that the standards applied are inappropriate, but that the current implementation is fundamentally flawed. As a result it is very difficult to support the bill which is currently making its way through the parliamentary process. Following a review and redesign of the regulatory regime, a very different set of powers may be more appropriate.

16. Turning, now, to the role of the regulator. There is an argument that the regulator exists in the wrong government department. As part of the Home Office, there is a natural tendency for the regulator to concentrate on the use of science for the investigation and subsequent prosecution of crime. It should be borne in mind that forensic science has wider applications extending into civil and family law. Many techniques are also applicable in situations which may not lead to court (e.g. corporate investigations, paternity testing etc.). Consideration should be given to whether the regulator should actually fall under the remit of the Ministry of Justice where, perhaps, more emphasis would be given to the forensic element. The regulator would then be free to consider issues of admissibility rather than trying to produce a form of licensing regime which favours large organisations dealing with the same scientific methods over and over again at the expense of smaller innovative providers which cannot meet the costs currently in force. This might also have the effect of making accreditation of forensic science providers something which the judiciary and legal profession take a real interest in, instead of seeing it as purely peripheral issue as they seem to do now. (see also paragraphs, 8-10 above).

17. If some form of licensing is deemed appropriate, then there should be an easier route into the licence for small providers. Full accreditation, as noted above, is prohibitively expensive but there are other standards which are

compatible with those desired by the regulator. Certification against those standards would provide a degree of assurance, albeit at a perceived lower level, that small providers were complying with the spirit of the regulations whilst allowing them to develop their organisations to allow full accreditation after a period of adaptation. Currently, the system is "big bang" and smaller organisations are starting to move out of forensic science or close down completely rather than gambling on a bill for tens of thousands of pounds for an accreditation process that may see them being assessed as "not fit for purpose" by assessors whose judgment and competence seems questionable.

**Forensic Science Research Landscape**

18. In an academic context, Forensic Science is something of a "poor relation" for funding and assessment. Because it is applied science and has not had its own unit of assessment in the Research Assessment Exercise (RAE) or Research Excellence Framework (REF), leading Universities appear to struggle to understand the value and role that forensic science can bring to their portfolios. A side-effect of this is that people, like myself, who are respected in the practitioner community and who regularly assist with solving difficult problems are on academic contracts which prohibit applications for research funding and discourage publication in order to "game" the REF returns by taking us out of the pool of qualifying researchers. This means that many excellent researchers are discouraged from moving into forensic science and reduces the pool of potential researchers because it is no longer seen as career enhancing.

19. The research councils do not routinely issue calls for such highly applied scientific research and assessment panels may struggle when a researcher applies under another theme, leading to rejection of potentially significant projects in favour of something which is more "mainstream" - i.e. easier for the panel to match against the criteria. Again, this sends a message to researchers that forensic science is not a good career move for ambitious talented academics,. Those who have a passion for forensic science find that the best way they can make progress is to disguise their work, "piggy back" it onto another project, or undertake it as consultancy activity through casework, which may result in an embargo or prohibition on publication of their results.

20. Where funding is available, it tends to be at the technology demonstrator level, supported by agencies who have an immediate need for solutions to current problems, rather than encouraging scientists to think more about future requirements.

21. Additionally, particularly in the fields of computing, engineering and design, funding calls and development grants rarely, if ever, include any mention of forensic readiness - i.e. the design & implementation of products to make them easier to investigate in the event that they are used in the commission of crime or are subject to an attack themselves. This is not unique to these funding streams, of course, and results in new products which must be reverse-engineered before they can be considered as proper evidence sources, leading to delays and uncertainty about the correctness of the methods being used, as noted above.
22. There is a potential argument, therefore, that there is a need for a dedicated Forensic Science funding body. However, this ignores the fact that forensic science needs to draw on, and influence, the whole research community in order to find innovative solutions to existing and future problems. Instead of a single funding body, independent of all the others, it would seem more useful to have a co-ordinating body with research councils in particular, guaranteeing that forensic readiness & applicability should become included in all calls, and that a percentage of all funding should be committed to forensic science research specifically.

23. Private sector research and development should not be ignored. However it is important to note that while the "traditional" sciences can rely on the underlying basic science to show that new equipment, tools etc. are correct, the problem of secrecy within the reverse-engineering disciplines remains (see paragraph 6, above) with the associated issues this causes with evidence of correctness of methods. Private sector research and development also tends to seek solutions to current problems rather than encouraging more "blue sky" speculative activity which may have benefit in the much longer term.

**Digital Forensics**

24. I believe that most of the text above addresses most of the specific questions on digital forensics, with the summary answers being, "Yes", "No" and "No." respectively.

25. Governments, businesses, society and individuals have become increasingly reliant on digital technologies for day to day activities and this makes digital systems attractive as both targets of crime and sources of evidence for various activities. Even the simplest crime is now likely to involve at least one mobile phone with an associated cloud data store and multiple social media accounts. The rate at which new apps. are added to online stores, and the ease with which even novices can develop them has created a situation which is unmanageable through proliferation of different data formats and massive increases in the amount of data generated and stored by and about each person. It is impossible for investigators to keep pace. It is a current problem, not a future one.

26. The digital forensics community, as a whole, needs to work more closely together to co-ordinate properly funded research addressing both current and future problems, and it needs to work with the users of the evidence to help understand their needs and to help them understand the evidence that is and can be produced.

*1 September 2018*