Written evidence from Professor Peter Sommer (DIS0017)

Summary

This submission concentrates on the issues around the acquisition, handling, investigation and disclosure of evidence in digital form.

Some adjustments are required in the standard procedures for disclosure to take account of its particular features while preserving the essential aims of the disclosure regime.

Rates of pay for specialists operating in the publicly funded arena are substantially below those available in immediately competitive areas. This leads to problems of staff retention and recruitment and in turn to substantial delays in examining digital devices unless the circumstances are urgent.

The introduction of forensic science regulation, in principle a good thing, has been designed around the needs of traditional "wet" forensic science laboratories which carry out commoditised tests. The current scheme is unsuited to the practicalities of digital forensics where regulation would be better aimed at individuals rather than laboratories. The costs associated with current forensic science regulation act as a drain on the limited funding available for front-line digital forensics work.

Qualifications

I have been providing expert evidence in the digital domain for over 25 years covering most forms of serious crime and many forms of civil dispute as well. I act for both prosecution and defence, though with an emphasis on the latter. I am currently Professor of Digital Forensics at Birmingham City University, hold a visiting professorship at de Montford University and have had posts, lectured and/or examined at the London School of Economics, the Open University, Oxford University, Oxford Brookes University, Queen Mary University of London and the Defence Academy. I also have consulted for a variety of government and non-government departments and given evidence to parliamentary committees as well as acting as a specialist adviser, most recently on the draft Investigatory Powers Bill. During its existence I was the joint lead assessor for digital forensics at the Home Office-backed Council for the Registration of Forensic Practitioners and have also served on the digital forensics specialist group for the Forensic Science Regulator. A short form CV appears at appendix 1; more detail is available at www.pmsommer.com

Along with others in March-April 2017 I conducted a survey of attitudes towards ISO 17025 accreditation for digital forensics and its conclusions are a source for some of the comments made in this submission. (http://digital-evidence.expert/UK%20ISO%2017025%20Digital%20Forensics%20Survey%20April%202017.pdf)

Role of digital evidence in criminal justice – and associated problems

1. The particular qualities of evidence in digital form, as opposed to other types of evidence that are adduced in criminal cases, are the quantities that need to be

considered, its complexity, the volatility of the source material, and the rate of change in information technology and the social and commercial structures that are thereby derived. It includes data stored on computers, laptops, mobile phones and laptops, data stored in the cloud, records of activities on social media sites, and records created and held by large organisations such as telecommunications companies, financial institutions, transportation companies, commercial businesses and government ministries and other state entities. There are also the devices we interact with – bank cash machine ATMs, shop sale systems, restaurants, transport payment systems, when we use public wifi, when we use an Internet Service Provider, a website or social media service, when we conduct a search via Google and its rivals, when we get caught on CCTV, the more so if the CCTV is linked to Automatic Number Plate Recognition.

2. The importance of digital forensics parallels the importance of computers and digital devices in our lives. Police say that the *average* UK home contains 7.4 digital devices most of which contain stored files but also software, configuration and system data which can be interpreted. The smartphone in particular has its very intimate relationship with its owner 60/60/24/7/365 and is recording activities second by second. Others put the figure even higher, the Internet Advertising Bureau UK cites 8.3 devices per home and Gartner suggest that by 2020 each of us will have 5.1 connected devices *on our person.*

3. In terms of quantity: A relatively simple home PC can easily contain over 50,000 files if we include all the supporting files which make Windows "work", fonts, help files, and in-built games, but over 350,000 and more is not that unusual. If the average home contains 8 or more digital devices and for each the amount of locally stored data doubles every year or so think of the practicalities when the police are investigating a conspiracy in which every device associated with every alleged conspirator may be important as evidence of a "common purpose". Worse still consider what happens in corporate investigations where there may be large numbers of work stations and central servers and each member of staff sends out vast numbers of emails, memos, shared diary items and substantive documents.

4. In terms of rates of change in IT and inherent complexity: Over the last 20 years Windows has been through Windows 98, ME, XP, Vista, 7, 8, 8.1 and 10. Each time there have been significant changes under the hood in terms of how data is stored and activity recorded. As every Windows user knows, multiple updates appear once a week. New file-sharing protocols have appeared at 3-year intervals and social networking facilities such as Facebook and Twitter managed to attract multi-billion followers within five years of start-up. Major new versions of smart phone operating systems appear every 12 months or so – the iPhone's iOS dates from 2008 and is now at version 11. Android in a form in which most will recognize it dates from 2009; it is now on Version 8. Apps like Facebook and Snapchat change on a weekly basis.

5. But digital forensics is not limited to data stored on PCs and smartphones. Network forensics traces activity on the Internet and on corporate systems. The investigator has to be alert to hijacked IP addresses which disguise a perpetrator and use multiple methods to attribute activity to a possible defendant. Phones both fixed and mobile produce "communications data" of who called whom, when and for how long; mobile phones also generate "where", geolocation data. In the form of cellsite analysis this can show the movements over time of a phone and hence its owner. There are also

types of evidence that were analogue but are now digital, for example audio and video recordings, including those from CCTV.

Procedures for the acquisition handling and analysis of digital devices

6. In order to evaluate procedures which meet the overall aims of disclosure it is helpful to understand the practices involved in acquiring, handling and analysing digital devices. Data on digital devices of all kinds is highly volatile and there is a requirement to "freeze the scene" on a personal computer, mobile phone, tablet, corporate computer, or cloud service. A simple direct examination of a device will cause many changes which amount to contamination of the original. Procedures involving hardware, software and management actions have been evolved to achieve reliable evidence preservation. They are described in the *ACPO Good Practice Guide For Digital Evidence* (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf). [1]
7. What is produced is referred to as a forensic copy or forensic image. Work is then carried out on the copy, not the original, by a law enforcement technical investigator. The forensic copy provides authenticity, provenance and continuity. Multiple copies of the forensic copy can easily be made, including for the defence. Techniques for investigating includes keyword search, the reconstruction of databases including emails and social media, photo content search, and the use of hash files of known offending material such as that involved in child sexual exploitation and terrorism. The techniques also include the ability to recover deleted material and view areas on a hard disk or on a mobile phone which are normally hidden. "Link analysis" and its sub-set "contact chaining" can be used to correlate a number of different sources of digital evidence.
8. This will normally result in a series of exhibits and in the first instance a Streamlined Forensic Report. The hope is that some defendants will be willing to plead on this basis alone. The Streamlined Forensic Report will normally be passed over to an accused's lawyer. In the event that an accused is not prepared to plead the lawyer will want to know from his client the basis on which the digital evidence is to be challenged. Typical responses may include: "there are emails/messages/photos/documents the prosecution have not looked at but which cast a different light"; "others had access to the device, not my fingers on the keyboard"; "my device was hacked". Defence lawyers will then instruct their own expert. There may be a demand that the police/prosecution produce a full report referring to all the material considered and explanations for conclusions reached. Typical instructions to a defence expert will be first to test the technical work of the police and any drawn inferences and second to see how far the explanations and comments of the accused can be supported. At some point a defence lawyer is expected, as part of the court procedure, to produce a Defence Case Statement[2].
9. Because of the quantity of data to be examined it is unrealistic to expect a prosecution expert or technician to carry out an exhaustive examination of all the devices that might have been seized. This plainly creates a problem for the disclosure regime as it

[1] ACPO has of course now been replaced by NPCC and it seems likely that a new edition of this publication will become available.
[2] S 6A CPIA, 1996

is normally understood. However the solution is to make available to the defence copies of all the forensic images that have been created by the prosecution. It is then open to a defence expert to use tools very similar or identical to those used by the prosecution to carry out the instructions of a defence lawyer. This surely satisfies disclosure in every practical respect.

10. My own experience is that this procedure of providing forensic copies to the defence presents very little difficulty and indeed little cost is involved other than the data media upon which the copies are placed. Where it is considered that the contents of the forensic copies are "sensitive" (because they involve indecent images of children, confidential material or terrorist manuals for example) the usual arrangement is to require a defence expert to provide an appropriate undertaking. In exceptional circumstances this can be bolstered via a court order, breach of which would be a contempt of court.

11. However I understand that this procedure is often not followed in "lesser" cases. This is a matter the committee should examine further.

12. In terms of changes to the existing disclosure protocols I draw attention to *Judicial Protocol on The Disclosure of Unused Material In Criminal Cases* of December 2013[3] and in particular paragraph 13: "Judges should not allow the prosecution to avoid their statutory responsibility for reviewing the unused material by the expedient of permitting the defence to have access to (or providing the defence with copies of) the material listed in the schedules of non-sensitive unused prosecution material irrespective of whether it satisfies, wholly or in part, the relevant test for disclosure. Additionally, it is for the prosecutor to decide on the manner of disclosure, and it does not have to mirror the form in which the information was originally recorded."[4] Although one can understand the reasoning behind this requirement if it is confined to conventional print-out material there seems a very good case for revising it where digital evidence is involved. The defence is not prejudiced by having access to the forensic image as they will be using search tools in order to locate material of interest to them; moreover if the forensic image has been created properly and in accord with published procedures as noted above the forensic image provides provenance, continuity and integrity of evidence which would otherwise be absent.

Digital forensic practitioners and the structure of the profession within which they work

13. Digital forensic technicians are employed direct by law enforcement either as sworn police officers or civilians. Rates of pay for civilians vary between £23,000 per year to just under £50,000 for the highly experienced. The committee may wish to enquire about levels of staff retention and turnover. Considerable use is made of out-sourcing; routine basic work is made the subject of competitive tendering. Although this commercial process has the advantage of keeping prices low it also results in a separation between an investigating law enforcement officer and a technician and also the strong likelihood that if an investigating officer has failed in their specification of requirements to cover all of the opportunities the outsourced company will be unlikely to suggest new opportunities. The outsourced companies can include those who offer

[3] Available at; https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Protocols/Disclosure+Protocol.pdf

[4] See also : https://www.cps.gov.uk/legal-guidance/disclosure-attorney-generals-guidelines

the full spectrum of forensic science services and those who specialise in only one aspect, for example the examination of personal computers or cell site analysis. There are a large number of very small companies and sole traders, often staffed by former employees of the police, the military, the intelligence agencies and academia. Smaller companies often work from home offices and hence have lower overhead costs. The small companies and sole traders, because of their extensive experience, are often called upon to deal with the more complex, challenging and innovative investigations. The sole traders are usually unwilling to become employees of larger firms.

14. Defence solicitors tend to wish to source individual experts, indeed they must meet the court's requirements for expert evidence under Criminal Procedure Rule 19, and very often these are sole traders or from the small companies. Standard legal aid rates for digital forensics experts have been reduced to £72 an hour. This compares with rates in excess of £200 – £300 an hour for privately funded and civil work.
15. Private sector salaries for digital forensic specialists tend to start around £55,000 a year. It should be borne in mind that there is an easy transfer from digital forensics to civil e-disclosure and other aspects of technical cyber security consultancy where rates of pay can easily reach £80,000 a year.
16. The disparity between public sector and private sector pay creates problems of staff retention and hence staff quality. Much of my information is anecdotal but the committee should be in a position to initiate enquiries from the police.
17. The shortage of staff to carry out investigations usually results in considerable delays unless an enquiry is deemed urgent – involving a threat to life, terrorism, or live investigations. Six-month delays on the routine examination of personal computers, tablets and smart phones are common. Again the committee may wish to institute its own enquiries.
18. A consequence of the delays is that individual police officers and prosecutors may hope to dispense with full examinations of digital devices and the associated requirements for disclosure.
19. Defence solicitors are finding it increasingly difficult to source experts willing to accept legal aid rates. The consequence here is that law enforcement work may not be properly challenged.

Impact of Forensic Science Regulation and ISO 17025

20. A third area the committee needs to consider in terms of effective and timely disclosure is the clumsy implementation of forensic science regulation in the digital forensics arena. Forensic science regulation was introduced as a quasi-replacement for the Forensic Science Service which was closed in 2012. The fundamental idea is a good one, to improve standards. However the design has been around the work of conventional forensic science laboratories which carry out high volume standardised tests on such things as DNA, blood, paints and fibre recognition. The concerns are to deal with the quality of the tests, avoidance of contamination of original exhibits and reliability of record-keeping. What is being regulated under the chosen standard, ISO 17025, is laboratory procedures.

21. It should be noted that forensic science regulation is not an absolute guarantee of quality. The committee will be aware of the allegations around Randox

(http://www.independent.co.uk/news/uk/crime/forensic-labs-data-manipulation-criminal-convictions-doubt-randox-testing-services-investigation-a8066966.html) which holds ISO 17025 accreditation. Accreditation and inspection did not spot the financial difficulties of Key Forensic Services which lead to a multi-million pound police bail-out (https://www.thetimes.co.uk/article/police-foot-the-bill-after-collapse-of-forensics-firm-key-forensic-services-limited-bg5nbxkxt).

22. The scheme is ill suited to the requirements of digital forensics as described above. A digital forensic examination involves considering a large number of potential records and artefacts from several different sources, reconstruction of events and the ability to deal with the ever-changing landscape of hardware, software and commercial and social applications. At the moment the FSR scheme is limited to data acquisition and does not include any of the analytic techniques. It is difficult to see how the FSR's tool testing regime can be applied at all, or at speed to cope with the realities of IT innovation. The regulator wants statutory powers to compel accreditation and whether a technician or expert can be contracted within the criminal justice system.
23. Instead of accrediting laboratories it would be better to accredit individuals. In effect the best form of testing of the quality of their work is against the requirements of the existing Criminal Procedure Rule 19 and associated Practice Direction[5] which specifies the necessary contents of an expert report - together with peer review by an opposing expert.
24. In addition, the costs of assessment, both the preparation and assessor fees, are high and are better suited to laboratories with high volume work. But for more specialist companies the costs of accreditation are particularly high as a proportion of their overall turnover, the more so as many of their key skills are not actually being assessed under the scheme. These costs must be paid for out of existing fees and hence are a deterrent to their continuing to offer services to the criminal justice system. It should also be noted that law enforcement agencies are having to pay assessment costs out of existing funds, and by diverting resources from frontline investigations.
25. Although the general aims of forensic science regulation are good the particular implementation in terms of digital forensics is having the effect of reducing the number of digital forensics experts available as they vacate the arena in favour of more financially satisfactory activity. Some specialist skills, for example, involving the compromise of ATMs and point-of-sale terminals, are being lost altogether.
26. I would be happy to expand on any of the issues raised in this submission either by further submission or by oral appearance.

Peter Sommer

19 March 2017

Appendix 1

[5] https://www.justice.gov.uk/courts/procedure-rules/criminal/docs/2015/crim-proc-rules-2015-part-19.pdf; https://www.justice.gov.uk/courts/procedure-rules/criminal/practice-direction/2015/crim-practice-directions-V-evidence-2015.pdf

Professor Peter Sommer combines academic and public policy work with commercial cyber security consultancy, with a strong bias towards legal issues.

His first degree is in law, from Oxford University. He is currently a part-time Professor of Digital Evidence at Birmingham City University and a Visiting Professor at de Montfort University. Until 2011 he was a Visiting Professor in the Department of Management at the London School of Economics. He has consulted for OECD, UN, European Commission, UK Cabinet Office Scientific Advisory Panel on Emergency Response, UK National Audit Office, Audit Commission, and the Home Office. He has carried out external audits of the Internet Watch Foundation hotline. The OECD work, written with Ian Brown, addressed the cyber aspects of Future Global Threats He has given evidence to the Home Affairs and Science & Technology Select Committees, the Joint Committee on the Communications Data Bill and to the Intelligence and Security Committee. He was a Specialist Advisor to the old Trade and Industry Select Committee and to the Joint Committee on the Draft Investigatory Powers Bill (now an Act).

During its existence he was the joint lead assessor for the digital speciality at the Home Office-sponsored Council for the Registration of Forensic Practitioners and has advised the UK Forensic Science Regulator and the Home Office on communications data.

He has acted as an expert in many important criminal and civil court proceedings in the UK and international courts usually where digital evidence has been an issue including Official Secrets, terrorism, state corruption, assassination, global hacking, DDoS attacks, murder, corporate fraud, privacy, defamation, breach of contract, professional regulatory proceedings, harassment, allegations against the UK military in Iraq, "revenge porn" on social media and child sexual abuse. Particular themes have been situations where technologies need to be interpreted in legal terms and assessments of quantum and extent of damage.

He is the author, pseudonymously, of The Hacker's Handbook, DataTheft and The Industrial Espionage Handbook, and under his own name, Digital Evidence, Digital Investigations and E-Disclosure (IAAC) now in its 4th edition and the Digital Evidence Handbook.

He is a Fellow of the British Computer Society and also a Fellow of the Royal Society of Arts.

A full CV is available at: http://www.pmsommer.com/PMSCV2017.pdf