Dr Suzanne Harkins, Harkins and Associates, Inc. – Written evidence (FRS0047)

Introduction

1. Harkins & Associates, Inc. is a technology consulting and software company with more than 50 years of experience in writing applications for and consulting on enterprise computing systems across multiple industries. Its Founder, Paul Harkins, developed and patented[1] a software code auditing tool, the Real-Time Program Audit (RTPA)[2], that generates an automated electronic audit record of a computer program. The resulting audit record has the ability to provide both historical and real-time data that records and reveals what has happened inside computer programs at executing program statement level.

2. This written evidence has been prepared by Harkins & Associates, Inc.'s CEO, Dr. Suzanne Harkins. While representative of the author's opinion alone, it is written from the perspective of a small business with a technology tool relevant to digital forensic science. Harkins & Associates, Inc. has offices in Philadelphia, USA and London, UK.

3. Harkins & Associates, Inc. welcomes the Select Committee on Forensic Evidence inquiry and the opportunity to submit written evidence. Of particular interest and import is the inquiry's focus on justice, the understanding and use of forensic evidence in the criminal justice system, and how evidence can be used throughout the justice process. The role of technology in the justice process has never been more important, and will only continue to grow in the future.

4. Many of the themes intermingle, however this submission focuses on two of the Inquiry's themes: (a) the Forensic Science Research Landscape, and (b) Digital Forensics. While the majority of points made refer to the general use of digital forensics, as suggested by the *House of Lords Call for Evidence* a practical example is on occasion referred to, namely the topic of financial fraud, and specifically the case of the *Securities Investor Protection Corporation v. Bernard L. Madoff Investment Securities LLC Adv. Pro. No 08-01789 (BRL)*[3].

5. The effective and robust use of forensic science to deliver justice in the UK and to solve crimes is unquestionably a worthy pursuit. However, the attention to and strengthening of resources for digital forensic science also offers other potential opportunities, for example: to bolster the UK's position as an international hub of finance through the prevention or prosecution of financial crimes such as fraud; the future prosecution of cybercrime[4] in the UK; to build upon the UK's reputation as the

---

[1] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=6,775,827.PN.&OS=PN/6,775,827&RS=PN/6,775,827

[2] See www.realtimeprogramaudit.com

[3] http://www.madofftrustee.com/document/dockets/006767-merkindeclarartion09-01182docket296.pdf

[4] https://www.ft.com/content/d56d8c42-ac2b-11e7-beba-5521c713abf4

international centre of FinTech innovation; as well as overlapping AI and data aims of the HM Government *Industrial Challenge*[5].

Understanding Forensic Science/Forensic Science Research Landscape

6. *Question 4: How can the Criminal Justice System be equipped with robust, accurate and transparent forensic science? What channels of communication are needed between scientists, lawyers and the judiciary?*

7. *Question 12: How should further research funding for forensic science be justified? What should be the focus of such research? What is the role of UK Research and Innovation, especially considering the interdisciplinary nature of much forensic science?*

8. Questions 4 and 12 are answered together.

9. One clear area of import, especially as the automation and digitisation of everyday services increases, is the communication and understanding of technical concepts to make them more easily understood by the relevant actors across the spectrum of the justice process.

10. As such, one suggested area of research is on the topic of effective communication of digital forensics technology concepts between stakeholders across the spectrum of participants in the digital forensics research, evidence gathering, and legislative processes. Attention to AI and its inevitable expanding role in everyday life has to some extent highlighted the concept of making technological concepts 'explainable'[6], and this topic should be narrowed for a more forensic science focus.

11. The author's position on interdisciplinary research is that it is frequently the most insightful, interesting and fruitful type of research – and also the most challenging. However academic discipline, preferred research methodology, or 'practitioner language' (eg, technical, legal, commercial), should not be a barrier to effective collaboration for the delivery of justice. The same can be said for organisation type. Thus it is suggested that both interdisciplinary research as well as consortiums comprised of different organisation types are supported with funding in the future. It is strongly suggested that the consortia model adopted in the recent Innovate UK funding scheme on *Transforming Accountancy, Insurance and Legal Services with AI and Data*[7] be repeated, and the topic itself either repeated or further refined to focus on digital forensics and/or financial fraud. The multi-disciplinary role of UK Research and Innovation is thus vital.

12. The bringing together of experts on the regulatory side of digital forensic science technologies will also be vital as questions relating to privacy, liability, control, transparency, ethics, and regulatory compliance will

---

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf

[6] https://www.accenture.com/us-en/blogs/blogs-why-explainable-ai-must-central-responsible-ai

[7] https://apply-for-innovation-funding.service.gov.uk/competition/169/overview

inevitably be important, as well as the balancing of public and private business interests.

13. Finally, support for small businesses and start-ups to research this topic should also be supported, particularly as relevant expertise is often necessarily located in smaller and more agile organisations.

14. *Questions 14: How can a culture of innovation in forensic science be developed and sustained?*
To state that 'innovation is important' in today's world is stating the obvious, or at the very least repeating the in-fashion obligatory catchphrase. The development and implementation of true innovation in practice means both imagining and developing sometimes radical new ways of business-as-usual, and then also addressing and overcoming barriers to adoption, whether the innovation is a step change or a radical overhaul.

15. What is clear is that the first step towards creating better, more efficient digital forensic tools and justice system, is that they first must be imagined, and then provided spaces for new ideas to incubate and technical details explored (eg, a sandbox environment). For example, from a digital forensics perspective, it is possible to imagine a world where all computer programs had automated code auditing showing exactly what happened in the computer program, including in real-time.

16. Great ideas often come from unexpected places; the support and funding of SMEs is a vital part of this culture of innovation, as well as forensic science.

Digital Forensics

17. *Question 16: Are there gaps in the current evidence base for digital evidence detection, recovery, integrity, storage, and interpretation?*

18. Key gaps in the digital forensics evidence base discussed in this submission relate to:
    (1) The temporal nature of technical data collection, and its potential effect on evidence gathering and crime prevention;
    (2) Types of technology, specifically 'legacy systems', and implications on where funds and attention should be directed; and
    (3) The Black Box, Data Flows, and Algorithm Manipulation

19. <u>Practical Example: The Bernard L. Madoff Ponzi Scheme</u>
In the introduction to *The Government Counter Fraud Profession: Protecting Public Services and Fighting Economic Crime*[8], Board Chair Mark Cheeseman notes that fraud is a 'constant threat' and 'a hidden crime which evolves quickly'. While this is undeniably true, fraud is also a threat that can evolve slowly, facilitated by a lack of tools to identify, produce

[8] Government Counter Fraud Profession. 2018 (July). The Government Counter Fraud Profession: Protecting Public Services and Fighting Economic Crime, Version 2.4. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730050/Annex_B_-_GCFP_Brochure.pdf

evidence for, and efficiently prosecute it. An example is the Bernard Madoff Ponzi scheme, which ran from at least the 1970s to 2008[9], was seemingly not flagged by regulators despite regulatory oversight[10], and ultimately defrauded its investors of approximately $20 billion[11]. As of 14 August 2018, the trustee recovery effort has recovered $13.3 billion over the period 2009 – 2018 and is still ongoing[12], a long and costly judicial process by any standard.

20. A closer look at the prosecuting evidence of the Madoff Trustee case[13] highlights: (1) temporal issues related to collecting digital forensic evidence (and its possible prevention in the future); and (2) the specificity of the technology itself, and the skills necessary for data collection, preparation, and interpretation.

The Role of Digital Forensic Science Tools in the Past, Present and Future:

21. There is a role for technology in past, present and future digital forensic activities, for example:

22. The PAST: The need for effective digital forensic tools for the collection of evidence in past events is clear. For complex crimes such as the Bernie Madoff Ponzi scheme, the scope of tools required, and the analytical and data gathering techniques necessitated to build evidence for an effective legal case, is immense. Given the sheer volume of technical data in large and complex cases, methodologies such as predictive modelling, sampling, and the use of computer algorithms to interrogate data are common. However such analytical techniques are sometimes used because of the simple absence of a tool to automatically generate code auditing.

23. While the ever increasing amount of available data provides challenges for forensic professionals, it also has the opportunity to create solutions. Through its provision of automated novel data production at executing program statement level, the Real-Time Program Audit (RTPA) is potentially such a tool.

24. The PRESENT: Advances in technology also offer opportunities to provide novel types of 'red flags' for auditors and regulators, creating real-time systems to prevent and immediately flag suspicious activity based on software code auditing. With appropriate regulatory, privacy, ethical and other safeguards in place, cloud technologies could be utilised to create dramatically-enhanced real-time regulatory oversight capabilities based on real-time source code auditing.[14]

---

[9] http://www.madofftrustee.com/document/dockets/006767-merkindeclarartion09-01182docket296.pdf
[10] https://en.wikipedia.org/wiki/Bernard_Madoff#cite_note-NoOne-74
[11] http://www.madofftrustee.com/trustee-message-02.html
[12] http://www.madofftrustee.com/recovery-chart-34.html
[13] http://www.madofftrustee.com/document/dockets/006767-merkindeclarartion09-01182docket296.pdf
[14] Harkins, Paul. On-Demand Forensic Accounting and Analytics. http://www.realtimeprogramaudit.com/wp-content/uploads/2016/08/Forensic-Accounting-White-Paper.pdf

25. The FUTURE: How technology will develop in the future is unknown, and as such regulation will always be to some degree catching up with technological developments. However much like a security camera may deter crime if people know they are being filmed, it is possible that the video-camera-like capabilities of code auditing and other technical tools could deter some types of crime in the future.

Which Technology? Which Skills?

26. The Madoff Trustee case highlights the plurality of technologies examined and from which evidence was collected, dating back to systems from the 1970s, including code written in languages such as RPG 36 and RPG II. While it is certainly true that many enterprises still use these systems and technologies to run their businesses, older coding languages and systems such as the AS/400 are not the typical targets for innovation or funding projects. Moreover, the number of programmers and pool of human resources with knowledge of them continues to shrink. Mainframe and other technologies grouped into the 'legacy system' category receive scant attention and are certainly not typical targets for the receipt of funding or innovation projects, yet they continue to be a fundamental component of the financial and other industries.

27. The Madoff case highlights the importance of digital forensic science tools for such legacy technologies, as well as the need to preserve skills to conduct investigations on them for historic cases going back several decades, but also for the prosecution of present-day fraud and other financial crimes.

28. The above comments do not, however, negate the importance and need for rigorous understanding and analytical techniques for new and emerging technologies, or big data systems.

The Black Box, Data Flows, and Fraudulent Algorithms

29. As the technology that underpins our lives and services becomes seemly more and more esoteric to the naked human eye, appropriate technologies must be developed, utilised, and regulated to monitor, flag, investigate, and provide evidence for when things go wrong. The ability to find attribution and identify data flows, including meta data and data lineage, is imperative. Providing insight into the existing and future 'black boxes' of technology is now a fundamental requirement for the provision of justice, and this seems only likely to increase in the future.

14 September 2018