Artificial Intelligence and Evidence

Seminars in Law and Technology (SLATE III), Singapore, 15 September 2021

Lord Sales, Justice of the UK Supreme Court[1]

INTRODUCTORY COMMENTS

1. It is a great pleasure for me to speak to you today, albeit by virtual means. The paper by Professor Seng and Mr Mason[2] constitutes a significant development in an area which is becoming increasingly important – how our laws of evidence might need to evolve in order to treat material appropriately which is generated by artificial intelligence and/or machine learning systems. In the time available to me today, I do not intend to repeat the arguments that are already comprehensively discussed in the paper. I will first set out what I mean by the term 'artificial intelligence'. I will then draw on the large body of work from the authors in this area[3] in order to set out the current position in UK law on electronic evidence more widely, and the extent to which our legal system has started to acknowledge the potential impacts of artificial intelligence in this area. I will provide some further thoughts on the issues that artificial intelligence poses for the laws surrounding the treatment of evidence, as well as some potential ways forward.

ARTIFICIAL INTELLIGENCE: A DEFINITION

2. Any discussion which involves artificial intelligence must start with a definition of that term. I am using the words as a shorthand for self-directed and self-adaptive computer activity. It arises where computer systems perform more complex tasks which previously required human intelligence and the application of on-the-spot judgment, such as driving a car. In some cases, artificial intelligence involves machine learning, whereby an algorithm optimises its responses through experience as embodied in large amounts of data, with limited or no human interference.

[1] I am indebted to my Judicial Assistant, Anisa Kassamali, for her assistance in preparing this paper.
[2] Daniel Seng and Stephen Mason, "Artificial Intelligence and Evidence" (2021) 33 SAcLJ 241.
[3] See, for example, Stephen Mason and Daniel Seng (eds.), *Electronic Evidence and Electronic Signatures* (5th ed., Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021)

It involves machines which are capable of analysing situations and learning for themselves and then generating answers which may not even be foreseen or controlled by their programmers. It arises from algorithmic programming but due to the complexity of the processes it carries out, the outcome of the programming cannot be predicted by humans, however well informed.[4]

3. For the purposes of this talk, I draw a conceptual distinction between algorithmic analysis on the one hand and artificial intelligence on the other - although I acknowledge that it is difficult to draw a clear dividing line between the two in practice. An algorithm is a process or set of rules to be followed in problem-solving. It is a structured process which proceeds in logical steps. Even when programmed into and performed by a computer, an algorithm does not necessarily preclude human input.

4. This understanding of artificial intelligence broadly accords with that set out in the paper. Professor Seng and Mr Mason describe it as "a system that acts intelligently by doing what is appropriate for the circumstances and the purposes assigned to it, including behaving flexibly in changing environments and objectives, learning from experience and making appropriate choices given perceptual limitations and finite computation".[5]

5. Most relevant to our discussion today are the AI systems which produce the evidence which we consider in the context of legal proceedings. These systems can be found in a variety of places. For instance, police might use automated facial recognition technologies which are then relied upon in the context of criminal proceedings. Separately, lawyers might use an AI system in order to streamline the often lengthy processes by which electronic data is identified, collected, and produced in response to a request for evidence in civil or criminal proceedings. As a shorthand,

[4] For further discussion, see Philip Sales, "Algorithms, Artificial Intelligence and the Law", Judicial Review, 25:1 (202), 46-66.
[5] Seng and Mason (n. 2), para 1.

I will refer to this as "**AI-generated evidence**" throughout this presentation, although in reality it might be the case that AI systems have only partially contributed to the creation of the relevant evidence.

EXISTING LEGAL FRAMEWORK IN THE UK

6. The starting point is that the UK's legal system, like that of Singapore, has not yet fully established how best to treat AI-generated evidence. When is it admissible in a court of law? What weight should it be given? Does the position differ depending on whether the proceedings are civil or criminal?

7. Relevant statutes and case law on the admissibility of evidence do not specifically reference AI-generated evidence and have not answered these questions. That being said, the UK statute book does not exhaustively set out how the wider category of electronic evidence, which has been prevalent for many years now, should be treated either. The rules on the admissibility of electronic evidence in the UK have largely been developed through the definition and redefinition of malleable rules on evidence. As they have arisen before the courts, various rules and legal devices have emerged in respect of, for instance, electronic signatures, emails, printouts, video records etc.

8. I do not intend to use up our time today by detailing these various developments in the UK legal system. Very briefly, the position in respect of evidence, including electronic evidence, in the UK is as follows.

9. In order to be admissible, electronic evidence must be authentic and (to some extent) reliable. Authentication occurs when evidence is identified as being what it purports to be. One has to satisfy the court that (a) the contents of the record have remained unchanged, (b) that the

information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate.

10. The authenticity of the evidence is a condition precedent to its admissibility. There are a number of factors which could establish authenticity, including testimony of a witness with knowledge, circumstantial evidence, and evidence describing a process or system that shows that it produces an accurate result. Where evidence from a computer or other digital device is concerned, challenges to the authenticity of evidence might take a number of forms. For instance, it might be claimed that records were altered, manipulated, or damaged between the time they were created and the time they appear in court as evidence. Or the identity of the author might be in dispute. The person responsible for writing a text or email might dispute that they wrote the text, or sufficient evidence might not be adduced to demonstrate the nexus between the evidence and the person responsible for writing the communication.[6]

11. Reliability: There is a presumption in English law that in the absence of evidence to the contrary, the courts will consider that mechanical instruments were in order at the material time. This common law presumption has prevailed, at least in criminal proceedings, since the repeal of section 69 of the Police and Criminal Evidence Act 1984 by section 60 of the Youth Justice and Criminal Evidence Act 1999. The reasoning behind this was that, in a world where mechanical instruments such as computers were becoming increasingly common, a positive obligation to always prove that they were reliable and in order was overly onerous and an inefficient use of the courts' (as well as the parties') time and resources.

12. This is clearly a laudable aim. However, as Professor Seng and Mr Mason have observed in their paper, there is a risk that the UK courts' own assumed familiarity with computers means that the

[6] For discussion see Mason and Seng (n. 3), paras 2.36-2.39 and chapter 6.

presumption has been given too much weight. Ubiquity is not the same as reliability. They explain that these 'mechanical instruments' are becoming more complex and, as a result, are more susceptible to different types of failure. I will draw on (and admittedly oversimplify) the example of hardware and software to make the point. Hardware can almost be regarded as an inanimate machine or a receptacle for evidence. Software is the programme which instructs that hardware as to how it should operate. Together, hardware and software make up a computer system. However, the courts have often treated computers as if they are merely pieces of hardware (or perhaps more pertinently, a piece of paper). This approach erroneously ascribes greater reliability to these electronic devices than is perhaps justified. Professor Seng and Mr Mason explain that the combination of a hardware and a software system is often notoriously unreliable. They explain that, even before the development of what we are now starting to refer to as artificial intelligence, defects in software have been exceedingly common. As software and its interaction with hardware has become more complex, it has become less deterministic or predictable.[7]

AI-GENERATED EVIDENCE AND THE LAWS OF EVIDENCE

13. The existing tensions at the interface between electronic evidence and the laws of evidence are exacerbated by technological developments. We have already reached the point at which our electronic devices are not simply mechanical instruments which store analogue data. This trend is increasing with the development of artificial intelligence and machine learning. As Professor Seng and Mr Mason's paper tells us, the complexity of AI systems essentially takes the issue of proving or disproving the reliability of evidence produced by AI systems to the next level. AI systems based on machine learning are not just based on the knowledge (or human input) of their operators and programmers, but also the collective knowledge of patterns from training and test data drawn from diverse sources. Facial recognition algorithms consistently have lower matching accuracies on females, people who do not have white skin, and those in the age group of 18 to

[7] For further detail see Mason and Seng (n. 3), paras 5.66ff.

30, because they are heavily dependent on the datasets against which they are trained, and these groups are poorly represented in the datasets.[8] This has obvious implications for the reliability of any such AI-generated evidence which, for instance, identifies an individual at the scene of the crime using such technology.

14. What, then, is the solution to this? This is a vast topic on which I cannot hope to reach a conclusion within the course of this presentation. Professor Seng and Mr Mason's article proposes one very helpful solution: treating AI systems as the 'witness' in proceedings. They suggest that, just as a human witness will be subject to an examination as to his or her experience and qualifications, subjecting AI output to the scrutiny of the hearsay rule, or something akin to it, helps to tease out the embedded human assertions from the results sought to be admitted in evidence. If there is no opportunity for the relevant human assertions to be tested – for instance, if the automatically-produced analysis is to be relied on but the programmer who wrote the software that generated the analysis is not called to testify – the analysis becomes hearsay.[9]

15. I see the force in this suggestion. It is a solution which works within the current sphere of the laws concerning evidence. It extends and redefines our existing legal principles in order to keep up with technological developments in our society.

16. On the other hand, it also poses difficulties. It may not be realistic to expect the person who programmed a commonly used system to be available to give evidence in every case. So perhaps one should be thinking of substitute processes of authentication and critique, such as calling expert evidence to review and expose the presuppositions embedded in the programming. What

[8] Seng and Mason (n. 2), paras 18, 37; also, eg, 'Swiss student shows Twitter algorithm has bias to whiter, slimmer faces', *The Guardian*, 11 August 2021.
[9] Seng and Mason (n. 2), para 38.

seems important is that there should be means to challenge the evidence and to question the weight to be placed on it, rather than too readily treating it as reliable.

17. I also wonder whether more is needed, or is at least desirable. Our laws on evidence have already been stretched in order to deal with evidence generated by computers. The relevant legal framework was generated in a paper-based world, and it is all too clear that this world is no longer the reality. To stretch these laws even further in order to deal with AI-generated evidence is perhaps going too far.

18. I have previously spoken about the creation of an algorithm commission that might function as a form of expert independent regulator in respect of algorithmic programmes. I have also spoken about the need for legislative intervention in order to deal with artificial intelligence more broadly.[10]

19. I do not bring this up in order to suggest that we must set up a commission and immediately pass new legislation in order to deal with the issues raised by AI-generated evidence. I simply mention this in order to highlight the fact that it might be necessary at this stage to come up with new solutions from first principles.

20. In England, this might be a topic which is appropriate for consideration by the Law Commission, an independent statutory body set up in order to keep the law of England and Wales under review and to recommend reform where it is needed. It has already engaged with some of the legal issues raised by increasingly complex technologies. For example, it is currently considering smart contracts.[11] Its project is still at the consultation stage and so it has not yet made its

[10] See discussion on both issues in Sales (n. 4).
[11] Law Commission, "Smart contracts: current project status", accessible at https://www.lawcom.gov.uk/project/smart-contracts/.

recommendations. However, the way in which it defines its task indicates its direction of thinking: "*[t]here are questions about the circumstances in which a smart contract will be legally binding, how smart contracts are to be interpreted, how vitiating factors such as mistake can apply to smart contracts, and the remedies available where the smart contract does not perform as intended. The nascent state of the technology means that there are few, if any, tested solutions to the legal issues to which smart contracts give rise.*"

21. The Law Commission sometimes recommends that the Government pass legislation in order to deal with emerging and complex legal issues. My feeling is that this is something that may be necessary for the treatment of AI-generated evidence. Where the courts are being faced by evidence of a fundamentally different nature from that in previous decades, it is difficult for them to deal with all the issues which arise merely by seeking to adapt arguably outdated laws of evidence.

CONCLUDING COMMENTS

22. I have spent much of my time discussing the possible challenges that artificial intelligence poses for our laws of evidence. However, we must not forget the vast potential of artificial intelligence. In this sphere, at its best, it can produce reliable and authentic evidence which would not otherwise be available. This can assist judges in coming to the right outcome in cases. More broadly, artificial intelligence is already improving efficiency across many areas of human experience, and these gains can often be deployed towards socially useful activities. For example, online courts might improve access to justice and reduce the time and costs involved in dispute resolution.

23. Moreover, I do not think that AI-generated evidence fundamentally changes the role of courts once the evidence has been deemed admissible. The task of the courts remains the same – to use

the evidence before them, ascribing to it an appropriate degree of weight, in order to determine cases efficiently and fairly.