TOPICS

COMPETENCE
Ms Lynne Townley

The importance of the issue of competency of witnesses regarding the trustworthiness (or not) of digital data cannot be overstated. During the planning of this edition, the extent of the devastation caused by what has become known as the Post Office litigation scandal, where hundreds of sub-postmasters and sub-postmistresses in the UK were wrongly convicted over a period of over 20 years due to defects in the Post Office's computer system, was just becoming known. Tragically, expert evidence identifying systemic shortcomings had been discounted by the Post Office's own investigators. What approach then should courts take when scrutinising the competency of witnesses in cases involving electronic evidence?

AI, VERIFICATION AND THE IMPLICATIONS FOR EVIDENCE
Professor Burkhard Schafer

When DNA evidence was introduced in criminal proceedings, it triggered debate over whether quantification of match probabilities by expert witnesses unduly encroached into the territory of the jury. This presentation discusses whether a similar discussion should be started in the field of digital evidence. As programs with autonomous reasoning capacities are integrated into our lives, statements about the reliability and correct working of these systems have increased in legal importance, as the Post Office litigation scandal shows. What role, if any, should formal verification and similar proofs play in this environment, proofs that guarantee some relevant property of a computer program - typically that it will always behave (or not behave) in a certain manner?

AUTHENTICATION OF ELECTRONIC EVIDENCE
Professor Luciana Duranti

This presentation will talk about evidentiary authentication by discussing the concept of authenticity through time. It will introduce the concepts of identity and integrity, accuracy and reliability, and will show how authentication in the digital world will be increasingly based on circumstantial evidence—such as the system(s) in which a record has been stored through time—rather than on the electronic material submitted as evidence itself. In fact, we cannot preserve such material, but only our ability to re-produce or re-create it, and we need to distinguish between stored and manifested evidence and assess both separately. Ultimately, authentication might have to be an inference based on security.

AUTHENTICATION ISSUES IN RELATION TO DISTRIBUTED LEDGER TECHNOLOGIES AND CRYPTOASSETS
Dr Allison Stanfield

Distributed Ledger Technology (DLT) is used in blockchains using cryptographic algorithms as a method of authentication, most notably in cryptocurrencies. Non-fungible tokens (NFTs) and other blockchain-based tokens, are designed to verify ownership of a crypto asset. Where there are assets of value and money, there is crime and so thefts of crypto assets and money laundering have prospered. Where there is ownership of intangible property, there will be infringements of such ownership. Courts are now faced with accepting evidence from law enforcement, looking to prosecute such crimes, and private litigants seeking to prove intellectual property violations. Authentication issues in relation to these relatively new technologies will be examined in this presentation.

ENCRYPTED DATA
Ms Jessica Shurson

Any discussion about electronic evidence in the digital era must reference encryption. Criminal investigations may be frustrated by encryption, especially when encryption obscures the communications of criminal offenders. This presentation will discuss the encryption workarounds available to law enforcement, primarily under the laws of the United Kingdom and United States. The primary focus of the presentation is on compelled disclosure—that is, the state's legal authority to compel a person to decrypt data that they control, usually present on a device such a phone or computer. The presentation will also consider a state's capability to compel the assistance of third parties, such as service providers, to decrypt data.

PROOF
Dr Nigel Wilson

Proof of electronic evidence requires careful consideration and updated training. This presentation discusses the proof of electronic evidence, emphasising the challenges associated with proving a fact with electronic evidence, the need for accreditation and training of digital forensic experts, together with the validation of the technologies, systems and methodologies used and the need for the correct handling, preservation and analysis of electronic evidence in investigation processes to ensure reliability of proof. It also discusses how the probative value of the evidence can be affected and its reliability compromised when critical procedures or measures are not followed and how technological solutions can enhance the efficiency, accuracy and forensic reliability of such investigations.

PRESUMPTIONS
Mr Stephen Mason and Associate Professor Daniel Seng

While there is general concern amongst judges, lawyers and legal scholars that evidence in electronic form is not to be easily trusted, there is a presumption in England and Wales and in Singapore (s 116A, Evidence Act) that when a computer is in order at the material time, the evidence that the computer produces may be trusted. Unfortunately, this has been widely misapplied, leading to miscarriage of justice in the Post Office litigation. This session explores the scope of the presumption, explains why it has been misunderstood, and argues for a careful review and even reform to ensure that the law continues to take into account the dynamic and constantly developing changes in technology.

SILE Accredited CPD Activity

Public CPD Points: 2.5
Area: Civil Procedure
Training Level: Foundation

Participants who wish to obtain CPD Points are reminded that they must comply strictly with the Attendance Policy set out in the CPD Guidelines. For this activity, this includes logging in at the start of the webinar and logging out at the conclusion of the webinar in the manner required by the organiser, and not being away from the entire activity for more than 15 minutes. Participants who do not comply with the Attendance Policy will not be able to obtain CPD Points for attending the activity. Please refer to https://www.silecpdcentre.sg for more information.