Title: **Evidentiary Foundations**

Author: **Edward J. Imwinkelried**

Date and place of publication: **11 May 2020, New York**

Edition: **11th**

Publisher: **LexisNexis**

ISBN**: 978 1 5221 9267 1**

This is the eleventh edition of Professor Imwinkelried's text, with the first edition having been published in 1980. The text relates to the law in the United States only and aims to be a practical guide for law students and young lawyers, who wish to understand and learn to present evidence in court. In particular, the text is designed to demonstrate how to lay the foundation of the evidence when it is being offered for admission as evidence in legal proceedings.

The chapters include (1) introduction, (2) related procedures (such as motions to strike), (3) the competency of witnesses, (4) authentication, (5) legal irrelevance limitations on credibility evidence, (6) legal limitations on evidence that is relevant to the historical merits of the case, (7) privileges and similar doctrines, (8) the best evidence rule, (9) opinion evidence, (10) the hearsay rule, its exemptions and its exceptions and (11) substitutes for evidence. Each chapter explains legal doctrines and then provides examples of how to question a witness when attempting to establish the foundation for evidence through that witness. There are also examples of when and how to object to lines of questioning or to the evidence itself.

The chapter on authentication looks at some modern forms of digital evidence, such as print-outs from social media sites, web sites and text messages. Professor Imwinkelried refers to computer-generated evidence as a 'species of scientific evidence' and includes his 11 steps to authenticate 'computer records' ('the 11 Steps'), which were espoused in the fifth edition of the text: (1) the business uses a computer, (2) the computer is reliable, (3) the business has developed a procedure for inserted data into the computer, (4) the procedure has built-in safeguards to ensure accuracy and identify errors, (5) the business keeps the computer in a good state of repair, (6) the witness had the computer readout certain data, (7) the witness used the proper procedures to obtain the readout, (8) the computer was in working order at the time the witness obtained the readout, (9) the witness recognizes the exhibit as the readout, (10) the witness explains how he or she recognizes the readout and (11) if the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Although the 11 Steps were cited in and cited in *In Re Vee Vinhnee*, 336 B.R. 437 (9th Cir. BAP 2005) and later in *Lorraine v. Markel American Ins. Co*. 241 F.R.D. 534 (D. Md. 2007) ('*Lorraine v Markel*'), the 11 steps have been critiqued by some authors (Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), who query whether the reliability of computer evidence should be questioned, particularly in relation to software which is, and will continue to be, unreliable. Indeed, there does not appear to be any discussion about how to lay the foundation for evidence produced by software. Although the text is focussed on the USA, issues with the reliability of software has been the subject of conjecture in other jurisdictions (see, for example, *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB), [2019] 12 WLUK 208, *R v Cahill; R v Pugh* 14 October 2014, Crown Court at Cardiff, T20141094 and T20141061 before HHJ Crowther QC; see also Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', *Digital*

Evidence and Electronic Signature Law Review, 17 (2020) 1), and it would have been interesting to see the juxtaposition of such authorities in the backdrop of USA authorities.

The Professor concedes his 11 Steps are more useful for a computer system that used punch card technology, and goes on to highlight that networked computers are more commonly used today, and provides an example of how to lay the foundation for evidence from networked computers. However, today a large percentage of businesses store their records in the cloud, so it is more likely than not that lawyers will be seeking to lay the foundation of records obtained from cloud systems such as MS Office365 and Bloomberg. How to obtain such evidence and then laying the foundation when admitting it in legal proceedings, does not appear to have been canvassed in the text.

The author looks at ways to lay the foundation for authenticating email, including whether cryptography is used in transmitting messages. Digital signatures are also examined where these are used in unencrypted messages. While the Professor does outline the way in which digital signatures can work using public and private keys, how to lay the foundation in the event a person denies having digitally signed a document, is not easily understood. An examination of the ways in which authentication documents that have been signed using products such as DocuSign would have been helpful, particularly in light of legislation around the use of electronic signatures and authorities such as *IO Moonwalkers, Inc. v. Banc of Am. Merch. Servs., LLC* 814 S.E.2d 583 (N.C. Ct. App. 2018).

The 2017 amendments to the Federal Rules of Evidence are referred to, namely r 902(13) and (14), which allows for 'certified records generated by an electronic process or system' and 'certified data copied from an electronic device, storage medium or file' to be self-authenticating respectively. Authentication of printouts of records maintained on a blockchain is considered and provides an example of a witness providing testimony explaining how blockchain works. This is useful to assist non-technical readers to understand how blockchain works, particularly if they need to lead evidence concerning such technology and about which they may be unfamiliar.

Technologies such as voiceprints are examined, as is the use of sound spectrography experts, however interestingly there is no discussion about artificial intelligence, which is increasingly being used in everyday life, both personal and in business. It would have been useful to refer to Judge Grimm's explanation of how to authenticate evidence produced by software using artificial intelligence, by utilising the new sub-rules (13) and (14) in r 902 Federal Rules of Evidence (The Hon. Paul W. Grimm, New Evidence Rules and Artificial Intelligence, *The Litigator's Toolbox 45 No.* 1, The American Bar Association, 2018). Nor does there appear to be any mention of the Internet of Things, which comprise data collected by devices, which transmit such data to other devices including storage platforms. An example of such systems might be refrigerators' devices data about temperature fluctuations, which is then stored on a cloud site, or devices which monitor a patient's medication needs. Such data might be used in evidence where someone falls ill, for example due to food poisoning in the former example and due to the wrong level of medication being administered in the latter example. The way in which to lay the foundation for this new type of digital evidence would be welcomed.

Laying the foundation for audio recordings, photographs including enhanced photographs, motion pictures and videotapes, x-rays, automated surveillance cameras (the 'silent witness'), computer animations and simulations are considered throughout the text. Additionally, examples of how to question the witness through whom such evidence is being tendered are included.

There is a chapter on the best evidence rule, and although the concept of an 'original' is discussed, this can only be confined to hard copy documents, since the concept of an original becomes superfluous when considering digital records. However, there does not

appear to be an explanation of such digital duplicates and this would have been helpful for non-technical readers.

Overall, the book provides useful guidance to practitioners seeking to lay the foundation for certain types of evidence, and given the first edition of the book was published forty years ago, it has no doubt stood the test of time. An in-depth consideration of the foundation for evidence produced by software, given its inherent reliability, would have made for some interesting reading. Further, while an attempt has been made to include contemporary types of evidence, broadening this to cloud computing, artificial intelligence, the Internet of Things to name a few, would have made the text more complete.

Allison Stanfield

Title: **Fake Photos**

Author: **Hany Farid**

Date and place of publication: **2019, Cambridge, MA, United States of America**

Publisher: **MIT Press**

ISBN**: 978 0 262 53749 0**

Hany Farid is a professor specializing in the analysis of digital images. This book from the Essential Knowledge series seems to be a concise version of his technical handbook *Photo Forensics* and aims to give a layman's understanding of the underlying principles and primary techniques of digital image forensics.

Somewhat untraditionally, the introductory background chapter is included as the last part of the book and covers the basic physics and geometry of light moving from a physical scene and hitting a sensor which transforms it into an electronic signal. These concepts are repeated in the body of the book which deal with authentication techniques or more accurately, ways to detect possible tampering of digital photographs, as they do not prove image authenticity. Each section of the book describes a different technique for image analysis and they are grouped according to the technical skills required.

The simpler techniques are based on analysing metadata and using Reverse Image Search but also on applying geometric principles, perspective and light for identifying manipulations of images. Hany Farid also makes a diversion to discuss the removal of perspective distortion.

Intermediate techniques focus on image imperfections introduced by JPEG compression and discuss JPEG signatures and cloning. Additionally, the properties of objects depicted in photographs are used for building facial 3D models or using 3D scene reconstruction.

Advanced techniques handle topics such as double compression, resampling and noise patterns, the latter even being detectable for individual distinctive cameras. For the reader, this might bring up comparisons to fingerprints. Computer-generated content and advances in machine learning are only briefly mentioned, although these technologies can already imitate a person's voice and generate fake videos with the potential to create undetectable forgeries.

Hany Farid focuses mainly on the technical details and at times his book reads like a matter-of-fact maths textbook, which is not a complaint. He includes several examples from his own practice and while interesting, some more direct examples, references or case law would have been appreciated. The techniques described are meant for digital photographs and can all be used behind the computer, while other possibilities such as dealing with physical photographs or location research are not discussed.

To point out a minor grievance, the author often points to coloured objects or lines, both in captions as well as the body of the text, but uses black and white images. While coloured images are included as a double print on higher quality paper which makes up a separate section of the book, it makes it harder to follow than it should, as these examples are extremely

helpful and go together with the text. At least one coloured image is entirely missing (orange mirror, figure 1.17) and in a few cases, references are made to the wrong images (figures 1.17, 2.2).

Fake Photos is practical and worth the read even if only for the many easily usable simple techniques for detecting manipulations in digital images.

Tõnu Mets

Chapter 1 Techniques Requiring Minimal Technical Skill

Chapter 2 Techniques Requiring Intermediate Technical Skill

Chapter 3 Techniques Requiring Advanced Technical Skill

Chapter 4 Closing remarks

Chapter 5 Background

Book Reports – for information

Title: **Technology-Enhanced Methods of Money Laundering: Internet As Criminal Means**

Author: **Fausto Martin De Sanctis**

Date and place of publication**: 2019, Switzerland**

Publisher: **Springer**

Hardback ISBN: **978 3 030 18329 5**

Paperback ISBN: **978 3 030 18332 5**

eBook ISBN: **978 3 030 18330 1**

Title: **Algorithms and Law**

Editors: **Martin Ebers and Susana Navas**

Date and place of publication: **2020, Cambridge, United Kingdom**

Publisher: **Cambridge University Press**

Hardback ISBN: **978 1 108 42482 0**

eBook ISBN: **978 1 108 68085 1**