

### THIS SESSION IS POWERED BY BSKB



### Official Sponsor of FICPI in 2024 Claiming Tomorrow Today™





# Unmasking the Mirage: Navigating the Landscape of Fake Evidence in IP Proceedings



STRENGTHENING THE PRACTICE OF THE INDEPENDENT IP ATTORNEY

www.ficpi.org



### Introduction

Elia Sugrañes Sugrañes SLP, Spain









Elia Sugrañes
Spain



Doug Deeth
Canada



Sara Navarro
Joven
Spain



Sergio Rizzo Spain



### Unmasking the mirage: Navigating the landscape of fake evidence in IP proceedings

Sara Navarro Joven Elzaburu, Spain





## Unmasking the mirage: Navigating the landscape of fake evidence in IP proceedings

FICPI 22nd Open Forum - Madrid

Madrid, 26th September 2024

### Current scenario regarding evidentiary matters

- Technological progress has brought significant advancements but also challenges.
- Traditional means of evidence vs. digital means of evidence.
- Proliferation of technical tools that facilitate the generation of new evidence and alteration of existing evidence.





### LegalBackground

- EU: No IP-specific legislation.
- Each EU Member State operates under its own general legal framework, covering both, substantive and procedural aspects.
- Certain degree of harmonisation still, no specific rules on evidence in IP-proceedings nor specific treatment for forged evidence.
- Some organisations developed Convergence Programs that partially address this issue and provide valuable information.



### LegalBackground

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

CP12– Evidence in trademark appeal proceedings: common recommendations on filing, structure and presentation of evidence, and the treatment of confidential evidence. EUIPN, March 2021.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

CP10 – Criteria for assessing disclosure of designs on the Internet. EUIPN, April 2020.



### **Fundamentals**

- Evidence relates to different sources of information, which may be used to establish and prove facts in trademarks proceedings.
- **Genuineness** and **veracity** of evidence should mean that it is not falsified, subsequently amended, altered or forged.
- A **global examination** of these items of evidence implies that they should be assessed in the light of each other.
- EU: No legal doctrine such as the US Doctrine of Inequitable Conduct as regards Patent Law.





### Means of evidence

#### Traditional means of evidence

- Invoices and other commercial documents.
- Catalogues, advertisements.
- Materials from business fairs and conferences.
- Publications (press notes, magazines, scientific papers, books or encyclopedias).

- Samples (packages, labels, tags or simples of the goods concerned).
- Official and public documents.
- Witness statements, sworn or affirmed statements.
- Market surveys.
- Certifications, rankings and awards.



### Means of evidence

#### Digital means of evidence

- Extracts from social media (applications, programs and websites, such as blogs and social networking websites).
- Electronic databases.
- Website archives.
- Editable and non-editable databases.
- Website analytics (traffic analytics, reports and statistics).
- E-commerce platforms.
- Metadata.



### Admissibility and probative value of digital evidence (I)

Electronic means of evidence **shall not be denied legal effect nor admissibility** as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures, seals, time stamps or registered delivery services.

Regulation (EU) 910/2014 refers specifically to:

- Electronic signatures Article 25
- Electronic seals Article 35
- Electronic time stamps Article 41

- Electronic registered delivery services – Article 43
- Electronic documents Article 46



### Admissibility and probative value of digital evidence (II)

Regulation (EU) 910/2014 defines **trust service** as an electronic service, normally provided for remuneration, which consists of:

- The creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- The creation, verification and validation of certificates for website authentication; or
- The preservation of electronic signatures, seals or certificates related to those services;



### Admissibility and probative value of digital evidence (III)

**Trust service provider** is understood as a natural or legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.

A qualified trust service provider is understood as a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.

- Impact on the burden of proof.
- Principle of party disposition.
- Mutual recognition Free movement of goods and services.



### Evidentiary value of evidence

- Each item of evidence shall be given appropriate weighing according to its probative value.
- CP12 Recommendations:
  - Evidence bearing a date, or other elements added afterwards.
  - Inconsistencies between all items of evidence.
  - For assessing genuineness and veracity of evidence.
    - Capability of the person from whom evidence originates.
    - Circumstances of preparation.
    - To whom it is addressed.
    - Whether it seems from the content to be sound, sensible and reliable.



Doubts as to the veracity and genuineness of evidence?





### Means for calling into question genuineness and veracity of evidence (I)

- It depends on the competent Court or IP Office.
- No specific available defenses before EUIPO, SPTO and WIPO (UDRP Proceedings).
- Available defenses before Courts:
  - Cross-examination of the parties.
  - Examination of witnesses.
  - Assessment of public and private documents.
  - Judicial recognition.
  - Expert witness opinion.



### Means for calling into question genuineness and veracity of evidence (II)

#### Expert witness opinion

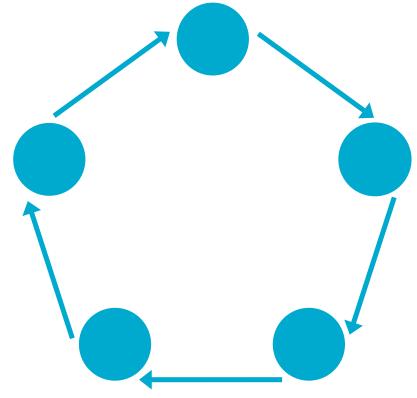
- On physical documental evidence Regular documentary witness opinión.
- On digital evidence Computer forensic witness opinion as regards:
  - E-mails without digital signature.
  - Analysis of computers and devices.
  - Identity theft and phishing.
  - Instant messaging or WhatsApp conversations.
  - Internet or web browsing history.
  - USB flash memories.
  - GPS data.



### Forgery

Altering any of the essential elements or requisites of a document.

Simulating all or part of a document, so as to lead to error concerning its authenticity.



Attributing declarations or statements other than those made to persons who intervened in a certain act.

Claiming intervention in an act by persons who were not part to it.

Untruthful narration of the facts.



### Forgery – Penalties under Spanish Crim in al Act

The Spanish Crim in al Act punishes forgery of:

- Public, official and business documents Articles 390 to 394 SCA
- Private documents Articles 395 and 396 SCA
- Certificates Articles 397 to 399 SCA
- Credit, debit cards and travelers' cheques Article 399 bis SCA

Different penalties depending on the subject:

- An authority or public officer while carrying out the duties of office Article 390 SCA
- Private in dividual Article 392 SCA



### **Statistics**

The Spanish National Statistics Institute published in 2022 a report on statistics as regards forgery.

	2022
18 Falsedades	
Total	7.292
18.2 Falsedades documentales	
Total	6.920
18.2.1 Falsificación documentos públicos	
Total	6.169
18.2.2 Falsificación documentos privados	
Total	468
18.2.3 Falsificación de certificados	
Total	240
18.2.4 Falsificación de tarjetas de crédito	
Total	43
18.99 Otros delitos de las falsedades	
Total	372

Available at: <a href="https://www.ine.es/jaxiT3/Tabla.htm?t=26016&L=0">https://www.ine.es/jaxiT3/Tabla.htm?t=26016&L=0</a>



### What occurs in practice?





### Example 1

Judgement of 16th November 2020 rendered by the Provincial Court of Madrid, Seventh Chamber, in Appeal proceeding No. 918/2020 [ECLI:ES:APM:2020:13089].

- Appeal brought against Judgement in Proceeding No. 278/2019,
   Madrid Criminal Court No. 20, re. forgery of a private document by a private individual.
- The appellant was accused of forging the signature of the owner of a Spanish national trademark and filing the assignment agreement with the Spanish Patent and Trademark Office.



#### 3<sup>rd</sup> LR:

"Constitutional jurisprudence and that of the Criminal Division of the Supreme Court have established that, in the absence of direct evidence, in some cases it is necessary to resort to circumstantial, indirect or indiciary evidence, the validity of which to undermine the presumption of innocence has been repeatedly admitted by both courts.

Through this type of evidence, it is possible to declare a principal fact proven by means of reasoning constructed on the basis of other facts, the indicia, which must meet a series of conditions, specifically that (i) the reasoning is based on factual elements and that these are several; (ii) that they are accredited; (iii) that they are interrelated and mutually reinforcing; and (iv) from a formal point of view, the inference must be considered reasonable and the judgement must express it, which does not imply the impossibility of other versions of the facts, so that the Court must have opted for the only possible certainty, but it does require that it does not opt for a factual occurrence based on a weak, inconsistent or excessively open inference (STC 175/2012 and STS 193/2013).



In turn, with regard to the crime of forgery, the case law of the Criminal Division of the Supreme Court (SSTS 627/2019, of 18 December, and 416/2017, of 8 June) has pointed out that 'it is not necessarily a type of own hand, so that several people can participate in the crime, collaboratively carrying out the action described by the type of crime, taking part in the execution, ideally participating in it, or assisting in its commission with necessary or accessory acts. In short, criminal participation is admissible in the offence of forgery, in any of the forms inherent to the concurrence of offenders.



On the basis of these premises, it is clear that the conclusion of the Criminal Court 'a quo' was based on a series of indications derived from validly obtained and practiced means of evidence, assessed by means of a judgement of inference with which, although the appellant may legitimately disagree, it can in no way be described as irrational, illogical or arbitrary, as it leads without forcing the rules of logic or the principles of experience to the direct or mediate authorship of the facts proved by the appellant, which excludes the viability of the allegation relating to the violation of the right to the presumption of innocence."



### Example 2

Judgement of 1 March 2023 of the General Court in Case T-552/21, Worldwide Brands, Inc. Zweigniederlassung Deutschland v EUIPO/Eric Guangyu Wan.

- Appeal brought against Decision of the First Board of Appeal in Case R 1548/2020-1, re. submission of a private investigator report to contradict evidence of use whose veracity was put into question in the course of a cancellation action on grounds of non-use.
- Parties to a proceeding are entitled to actively submit evidence that contradicts evidence whose genuineness and veracity is doubted.



"It must also be pointed out that, before the Cancellation Division, the applicant submitted an **investigators' report** that had been drawn up by an undertaking which had, inter alia, approached Detecami in Barcelona (Spain) and questioned one of its employees and also one of its representatives for central and north Spain in order to ascertain whether that company actually used the contested mark in connection with the sale of shirts." (p. 99)

"In response, the intervener submitted additional exhibit No 6, in which the employee questioned stated, inter alia, that the words which she had spoken and which had been recorded in the investigators' report submitted by the applicant had been taken out of context and that, as an employee of that company since September 1976 and the person in charge of the commercial management of the company's clothing sector since June 2015, she had never personally had to deal with the marketing of the contested mark in Spain." (p. 101)



"In that regard, it must be pointed out that the Board of Appeal stated, in paragraphs 72 and 73 of the contested decision, that it had taken into consideration that an overall assessment of the evidence had to be carried out taking into account all the relevant factors in the particular case and that, when making that assessment as to genuine use, it had to consider the evidence in its entirety and could not disregard some of it. (p. 102)

However, as is submitted by the applicant, the Board of Appeal did not state anywhere in the contested decision whether and how it had taken the investigators' report into account, just as it also did not, in the context of its assessment of the evidence, examine the declaration which the intervener had submitted in response (additional exhibit No 6). (p. 103)

The Board of Appeal was, however, required to base its decision on all the matters of fact and of law which the parties had submitted during the proceedings (judgment of 6 June 2018, *Uponor Innovation* v *EUIPO* – *Swep International (SMATRIX)*, T-264/17, not published, EU:T:2018:329, paragraph 80)." (p. 104)



### Practical recommendations

- Meticulous attention to detail when analyzing evidence submitted by the Counterpart.
- Actively using all available resources to highlight to decision-making Authorities any pieces of evidence suspected of manipulation or alteration.
- Whenever possible, rely on evidence provided by trusted service providers.





### Thanks for your attention.

Any questions?

Sara Navarro Joven – <u>snj@elzaburu.es</u> Abogada · Senior Associate Elzaburu SLP



### Unmasking the mirage: navigating the landscape of fake evidence in IP proceedings

Sergio Rizzo EUIPO, Spain





### **Unmasking the mirage:**

### navigating the landscape of fake evidence in IP proceedings



Sergio Rizzo
Member of the 3rd and 5th Boards of Appeal
EUIPO

FICPI 22nd Open Forum Madrid, 26 September 2024



#### Means of taking evidence before the EUIPO

#### NOT exhaustive list (Art. 97 EUTMR, 51 EUTMDR, 65 CDR and 43 CDIR):

- the production of documents and items of evidence
- requests for information
- sworn or affirmed statements in writing
- opinions by experts
- hearing the parties
- hearing witnesses
- inspection in situ



#### Some basic principles...

- In order to assess the evidential value of a document, it is necessary to verify the likelihood and the accuracy of the information which that document contains.
- It is necessary to take account of, inter alia, the origin of the document, the circumstances in which it came into being, the person to whom it was addressed and whether, on its face, the document appears to be sound and reliable.

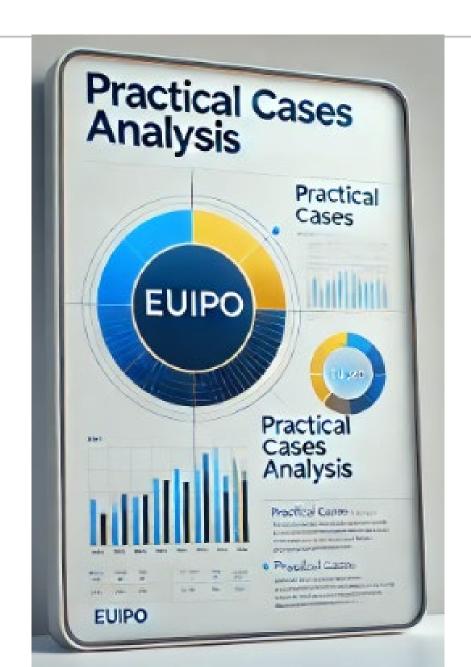
(08/05/2017, T-680/15, L'ECLAIREUR, § 72; 13/01/2011, T-28/09, Pine Tree, § 64; 07/06/2005, T-303/03, Salvita, § 42).



### Some basic principles...

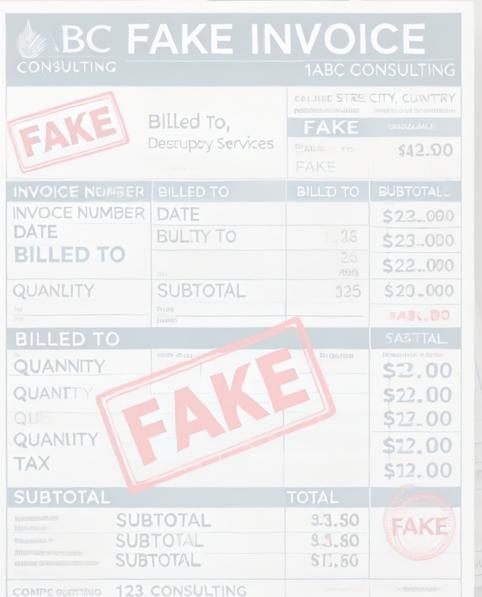
- The mere abstract and theoretical possibility that the content or date of evidence may be manipulated is not sufficient to undermine its credibility.
- Credibility can only be undermined by invoking concrete facts that suggest manipulation.
- Evidence of manipulation may include clear signs of falsification.
- Manifest contradictions in the information shown can suggest manipulation.
- Obvious inconsistencies that reasonably justify doubts as to the genuineness of the evidence may also indicate manipulation.













# 1<sup>st</sup> example



#### Invoice submitted in proceedings before the EUIPO



Sede Legale:

CORSO NOVARA, 40 - 80143 NAPOLI Tel. 081/731.39.65 - 081/461.28.97

Telefax 081/731.47.55

Cod. Fisc. e Part. IVA 07581111213

C.C.I.A.A. N. 895417

www.kenon.it

amministrazione@kenon.it



FATTURA / FATTURA D.D.T. / NOTA DI CREDITO (D.P.R. 472/96 DEL 14/8/96)

#### COPIA DI CORTESIA

Spett.le

PARTENOPE SERVIZI S.R.L.

VIA EDUARDO SCARFOGLIO. 7/G

80125 NAPOLI

NA

5444 40 15 9 08371021216 (27.742) (10/12/2018	
	1
CONDIZIONI DI PAGAMENTO.  23 RIMESSA DIRETTA **	n, de

CODICE ARTICOLO	DESCRIZIONE	U.M.	QUANT, CIFRE	PREZZO UNIT.	SC.1	SC. 2	IMPORTO NETTO	IVA
KREMINO	MISCELA KREMINO CONFEZIONE DA Kg.1	KG	21.00	21.00	35.71		283,52	22
NB	ZUCCHERO SEMOLATO IN BUSTINE	KG	10,00	1.40			14,00	10



#### **Original invoice**



Sede Legale: CORSO NOVARA, 40 - 80143 NAPOLI Tel. 081/731.39.65 - 081/461.28.97 Telefax 081/731.47.55 Cod. Fisc. e Part. IVA 07581111213 C.C.I.A.A. N. 895417 www.kenon.it amministrazione@kenon.it



\*X\*PANDENA / FATTURA D.D.T. \*\*NOTA BRIGINEDIRO (D.P.R. 472/96 DEL 14/8/96)

Spett.le

PARTENOPE SERVIZI S.R.L.

VIA EDUARDO SCARFOGLIO, 7/G

80125 NAPOLI

NΛ

DOD CLENT	N/A-	2CNA	AGENTE	CATEG	PARTEA IVA/CODICE FISCALE	NUMERO FATTURA	CATE PAGE	STREET, STREET
5444		40	15	9	08371021216	27.742	10/12/2018	1
23		SA DIRETT	A **		AIOTE.			

CODICE ARROOTO	DESCRIPTIONS	UMA	QUANT CIRE	PREZZO UNE	SC 1	SC. 2	MPORTO NETTO	MA
CM	MISCELA MAX BAR CONFEZIONE DA Kg.3	KG	21	21,00	35,7	1	283,52	22
NB	ZUCCHERO SEMOLATO IN BUSTINE	KG	10	1,40			14,00	10



#### Invoice submitted in proceedings before the EUIPO



Sede Legale:

CORSO NOVARA, 40 - 80143 NAPOLI Tel. 081/731.39.65 - 081/461.28.97 Telefax 081/731.47.55

Cod. Fisc. e Part. IVA 07581111213

C.C.I.A.A. N. 895417

www.kenon.it

amministrazione@kenon.it



FATTURA / FATTURA D.D.T. / NOTA DI CREDITO (D.P.R. 472/96 DEL 14/8/96)

#### COPIA DI CORTESIA

Spett.le LINDA SRL

COD. CLIENTE	IVA	ZONA	AGENTE	CATEG.	PARTITA IVA/CODICE FISCALE	NUMERO FATTURA	DATA PAG.
4014 CONDIZIONI DI PAG	CAMENTO		16	1	06962941214	404	08/01/2016
DOINDECH DI PAG	MINIENIO				NOTE		
22	RIMESS	SA DIRETT	A *				

CODICE ARTICOLO	DESCRIZIONE	U.M.	QUANT, CIFRE	PREZZO UNIT.	SC.1	SC. 2	IMPORTO NETTO	IVA
	THE RESIDENCE OF THE PARTY OF T		M. West In	BETT MOS	T M t	105 (3)	CHINES	
KREMINO	MISCELA KREMINO CONFEZIONE DA Kg.1	KG	30.00	15.50			465.00	22
001	CREMA DI NOCCIOLA G.1000 IN VETRO	No	5.00	22,00	13.64		95,00	10



#### **Original invoice**



Sede Legale:

CORSO NOVARA, 40 - 80143 NAPOLI Tel. 081/731.39.65 - 081/461.28.97

Telefax 081/731.47.55

Cod. Fisc. e Part. IVA 07581111213

C.C.I.A.A. N. 895417

www.kenon.it

amministrazione@kenon.it



\* FATTURA D.D.T. / NOTA DI CREDITO (D.P.R. 472/96 DEL 14/8/96)

Spett.le

LINDA SAS DI ORSINI ERMELINDA C.

VIA PONTE IZZO, 129

80045 POMPEI

MA

COD, CLIENTE IVA	ZONA	AGENTE	CATEG.	PARTITA IVA/CODICE FISCALE	NUMERO FATTURA	BAIA PAG.
4014	SEED IN CO	16	1	06962941214	404	08/01/2016
CONDIZIONI DI PAGAMENTO			The Marketon	NOTE	Control of the Contro	and the second second second
22 RIMES	SA DIRETI	* A				MUDICAL STANDARD TO THE

CODICE ARTICOLO	DESCRIZIONE	U.M.	QUANT. CIFRE	PREZZO UNIT.	SC.1	SC. 2	IMPORTO NETTO
CS	MISCELA SUPERMAX BAR CONF.DA Kg.3	KG	30,00	15,50			465,00
	Lotto R36A		YDAVIE	LA PER LA	TAN		
001	CREMA DI NOCCIOLA G.1000 IN VETRO	No	5,00	22,00	13-64		95.00



#### Additional evidence for further supporting the alleged manipulation

## KENON S.p.A.

U.O.L. VIA F.GRAZIANO 16 - 80022 ARZANO (NA)

Arzano li 02/01/2017

LISTINO PREZZI

#### MISCELE BAR

Miscela Baby Bar
Miscela Crema Moka
Miscela Crema Bar
Miscela Max Bar
Miscela Supermax Bar
Miscela Karamell 100% arabica

€ 15,00 per Kg. € 17,50 per Kg.

€ 17,50 per Kg. € 19,00 per Kg. € 21,00 per Kg.

€ 23,00 per Kg.

€ 24,00 per Kg.



# 2<sup>nd</sup> example

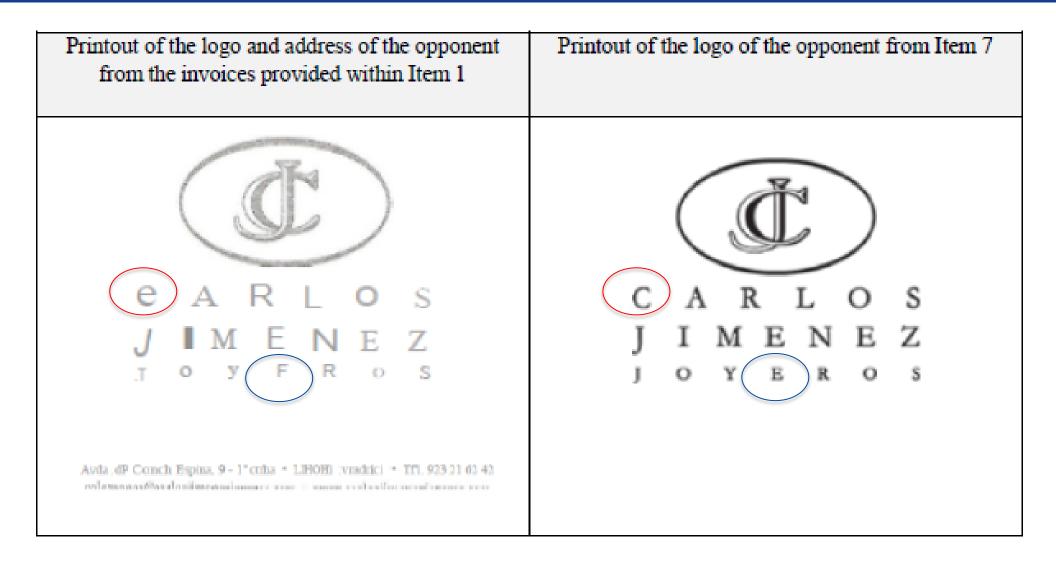


### R 1784/2019-4 of 12/02/2020

No.	Invoice No.	Date	Customer	Comment	Sum
1	17 487	15/02/2018	J. Lahidalga S.L., Madrid	(professional representative)	2 200,00 €
2	16 785	23/11/2017	Carolina Martin, Madrid	(partner of the professional)	3 500,00 €
3	16 934	28/12/2017	Carolina Martin, Madrid	(partner of the professional representative)	2 600,00 €
4	15 784	28/10/2016	Jessica Moragón, Madrid		500,00€
5	14 425	28/10/2015	Maria Antonia Perez, Madrid		1 975,00 €
6	10 045	28/05/2014	J. Lahidalga S.L., Madrid	(professional representative)	4 125,00 €
7	12 748	08/01/2013	J. Lahidalga S.L., Madrid	(professional representative)	1 100,00 €

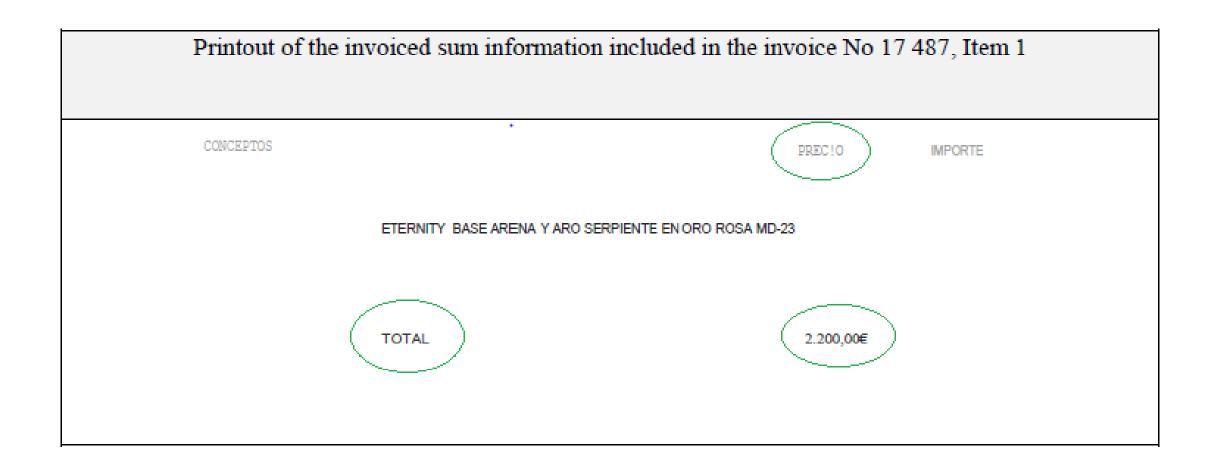


### **Unusual typing errors**





### Missing VAT details on invoices





# 3<sup>rd</sup> example



#### R 2089/2019-4 of 10/06/2020

 Inconsistent VAT rates: Some invoices applied different VAT rates before the official changes were implemented in Spain.



 Incorrect special tax on alcohol: All invoices applied a constant special tax on alcohol, which had actually changed multiple times between 2010 and 2017.



 Premature logo changes: The invoices featured the updated "PROHIBIDO" logo that was introduced only around 2014-2015.



 Header design: There were inconsistencies in the use of the old and new header designs across invoices dated before and after the official design change.









# 4<sup>th</sup> example



#### R 19/2016-4 of 26/04/2016



"It appears impossible that any billboard could have been placed at or close to this intersection, since it would have jeopardized the traffic".



### **Anomalies in the images**

1.4











#### **Inconsistencies**





"The billboards shown are not the same, the grasses next the billboards are different. On the left photo, a mast appears which is, however, missing on the right. In case that two billboards were placed, this would be contradicting the explanations of the respondent"



#### **Unusual shadows**





"the billboards do not cast shades at all or some billboards cast shades which are odd compared to the shades of other objects, such as cars"

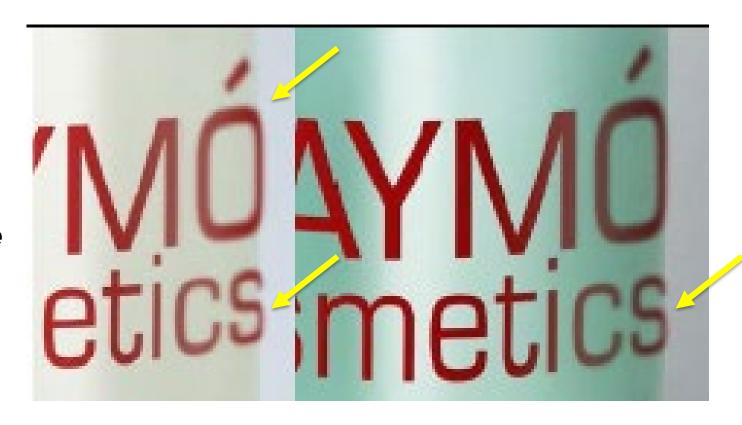


# 5<sup>th</sup> example



#### R 2278/2020 of 23/09/2021

"No forensic expert is needed to see that, at first glance, the contested mark seems to have been artificially placed on the bottle images".





### **Artificially blurred?**





### Inconsistencies: blurred transparent letters vs. focused non-transparent letters





#### **Inconsistent curvatures**





#### Consequences on the rest of the evidence presented

If false evidence has been presented, the rest of the evidence cannot be trusted either.

If the other evidence is genuine, why was there a need to present manipulated evidence?

Furthermore, if the goods and services are genuinely offered under the mark, the party could have provided genuine, unaltered photos instead of apparently falsified ones.





**Signatures** 





# 6<sup>th</sup> example



#### R 2052/2015 of 04/08/2017

COUTURE

LORIS AZZARO FARIS

NATURE UP Monsieur Jean Louis Daré 18, Boulevard des Minimes 31200 TOULOUSE AVOCATS
SPÉCIALISTE EN DROIT DE LA
PROPRIÉTÉ INTELLECTUSEL:
250 bis, rue du Feubauts Baint Honoré - 75008 PAR.;
Tél.:+88 (9) 1.44.05.00.00

1

Cormoctreuil, le 19 juin 2006

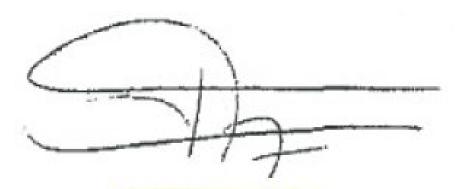
Monsieur Le Président et Cher Ami,

Suite à nos différents entretiens et à notre dernier courrier du 16 juin, je vous confirme que la Société LASA yous autorise à déposer et à exploiter la Marque AZZARO en classe 32 pour l'eau minérale afin de mieux financer l'Institut Loris Azzaro.

En espérant vous être agréable ;

Je vous prie de croire Monsieur Le Président et Cher Ami, à l'expression de mes meilleurs

Antoine FREY



Antoine FREY



#### DÉCISION INTÈRIME de la Première Chambre de recours du 4 août 2017

Dans l'affaire R 2052/2015-1

13 La Chambre considère important de connaître la véracité de la signature. Prenant en considération le fait que la titulaire de la MUE considère que la signature est celle de M. Antoine Frey, Directeur Général de LORIS AZARRO SAS en 2006, habilité à autoriser l'enregistrement de la marque au nom du propriétaire des droits au nom, mais que M Antoine Frey, qui a ultérieurement vendu son entreprise au groupe REIG CAPITAL GROUP sans communiquer qu'il avait autorisé à des tiers l'enregistrement de la marque « AZZARO » (voir paragraphe 9), est cité par la Cour d'appel de Paris du 20 janvier 2015 comme déclarant que la lettre portait « une imitation grossière de sa signature » (voir Annexe F (6), cité au paragraphe 6), il est prudent de connaître le résultat de l'investigation par l'instance pénale compétente. En particulier, dans le cas où il s'avèrerait que la signature était un faux et la titulaire de la MUE la victime de machinations malhonnêtes, il était prudent de ne pas utiliser la marque et une justification de non-usage aux termes de l'article 15 du RMUE ne semble pas être exclue par la Chambre.





Sergio RIZZO
Boards of Appeal
EUIPO



www.euipo.europa.eu



- @EU\_IPO
- in <u>EUIPO</u>
- **6** EUIPO.EU

# Thank you!



# Unmasking the mirage: navigating the landscape of fake evidence in IP proceedings

Doug Deeth DWW, Canada



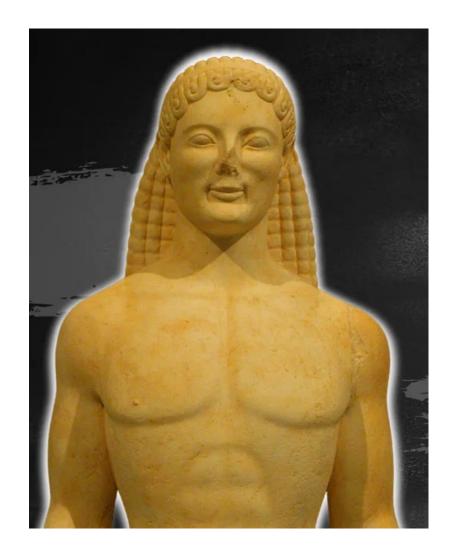


### There's always been fakes

"As long as there's been evidence in court, there's always been fakes, and the courts have come up with rules to deal with those as they come up, and are aware that there's always the possibility that somebody is trying to hoodwink them".

 "Courts and lawyers struggle with growing prevalence of deepfakes" (above), Riana Pfefferkorn, associate director of surveillance and cybersecurity at the Center for Internet and Society at Stanford Law School, states





### Fakes have always been with us

Dispute in Rome in about 223 AD over the authenticity of what was then sold as a 1000 year old Greek statute from Sparta.

berentur homines credere non au quodes
se uerum cerussima ratione docerentur
nhoc libro dixi inquib, tam legis preceptis
atq mandatis quib, nunc xpianos utisas non
est quale uel sabbatum est uel circucisio
uel sacrificia es siquid huius modiest tanta



## Risks of Deepfakes

Al created documents, images, videos and audio recordings are becoming more sophisticated and increasingly difficult to detect

Use of these documents can affect or even determine the decision in any administrative or contested proceeding

- If used in your evidence, even inadvertently, can damage or destroy the credibility of your witnesses
- Not always the "other side" that creates fake evidence

If used by the other side, and not detected, can result in a decision that is not only wrong but unappealable.



#### Admissibility of Real Evidence

#### What is this?

"Any evidence in which the Court acts as a witness, using its own senses to make observations and draw conclusions, rather than relying on the testimony of a witness"

Includes articles, observation of demeanour of witnesses (credible or not), audio and video recordings, and photographs.

#### Admissibility requires:

- 1. Prior testimonial evidence, or
- 2. Admission by the other party of its authenticity.

Common law courts have pre-trial procedures that allow parties to examine and agree on the admissibility of real evidence. For example:

- 1. that a video recording was taken at a certain time and by a certain camera, or
- 2. that a document was created or sent by one person to another,

without admitting that the contents of the document are true or that the video shows what one party says it shows.



#### Admissibility of Photographs and Videos

#### Three essential criteria

- 1. Accuracy in representing the facts;
- 2. Fairness and absence of any intention to mislead;
- 3. Verification on oath (of the above) by a person capable of doing so.

It is not necessary that the witness have taken the photo or operated the video camera. Videos and photos may come from an unattended surveillance camera, such as a video doorbell, with evidence to support the authenticity and accuracy of the video recording.

Concerns may arise from editing or other manipulation of the image.

Audio recordings are treated as evidence from a person who had overheard an conversation and made accurate notes.



## Admissibility of Electronic evidence

Authenticity can be established by proof of the integrity of the electronic documents system by or in which an electronic document is recorded or stored, including evidence:

- that at all material times the computer system or other similar device used was operating properly or, if it was not, that fact did not affect the integrity of the electronic document
- there are no other reasonable grounds to doubt its integrity;
- that the electronic document was recorded or stored by a party adverse in interest to the party seeking to introduce it (e.g. the other side's documents); or
- that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it.



#### Federal Rules of Evidence - USA

Two Federal Rules of Evidence, 902(13) and 902(14), aim to simplify the process of admitting videos and other electronic documents created with verified-capture tools.

Rule 902(13) allows for the authentication of a "record generated by an electronic process or system that produces an accurate result," if "shown by a certification of a qualified person" in a manner set forth by the rules.

Rule 902(14) allows for the authentication of "[d]ata copied from an electronic device ... by a process of digital identification, as shown by a certification of a qualified person."

Both rules require proponents to meet the notice requirements of Rule 902(11),

 "[b]efore the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them."

Common Law courts generally want to avoid surprises at trial.

Documents are commonly agreed upon, with specified limitations.



#### Are the existing rules good enough?

The US Judicial Conference's Advisory Committee on Evidence Rules, an eight-member panel responsible for drafting evidence-related amendments to the Federal Rules of Evidence, met in Washington, DC, in April 2024 to discuss the challenges of policing Algenerated evidence in court trials.

The potential risks of AI being used to manipulate images and videos or create deepfakes that could disrupt a trial were considered.

The agenda referred to deepfakes as follows:

A deepfake is an inauthentic audiovisual presentation prepared by software
programs using artificial intelligence. ... developments in AI make deepfakes much
more difficult to detect. Software for creating deepfakes is already freely available
online and fairly easy for anyone to use. As the software's usability and the videos'
apparent genuineness keep improving over time, it will become harder for
computer systems, much less lay jurors, to tell real from fake.



## Is there really a problem?

Some judges on the panel expressed skepticism about the urgency of the issue, noting that there have been few instances so far of judges being asked to exclude Algenerated evidence. One is quoted as saying:

• "I'm not sure that this is the crisis that it's been painted as, and I'm not sure that judges don't have the tools already to deal with this".

Chief US Supreme Court Justice John Roberts has acknowledged the potential benefits of AI for litigants and judges, while emphasizing the need for the judiciary to consider its proper uses in litigation.

Determining how the judiciary can best react to AI is apparently one of Roberts' priorities.



## Attempts to strengthen the rules (1)

The committee considered several deepfake-related rule changes, including a proposed modification of Federal Rule 901(b)(9), which involves authenticating or identifying evidence, to revise the Rule 901(b)(9) standard for admissible evidence from "accurate" to "reliable."

The new rule would read as follows (additions in bold):

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.



# Attempts to strengthen the rules (2)

(b) Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement:

....

- (9) Evidence About a Process or System.
- (A) evidence describing it and showing that it produces an accurate a valid and reliable result; and
- (B) if the proponent concedes that the item was generated by artificial intelligence, additional evidence that:
  - (i) describes the software or program that was used; and
  - (ii) shows that it produced valid and reliable results in this instance.



# Attempts to strengthen the rules (3)

The committee also recommended the addition of a new rule, 901(c), which was initially proposed as:

901(c): Potentially Fabricated or Altered Electronic Evidence. If a party challenging
the authenticity of computer-generated or other electronic evidence demonstrates
to the court that it is more likely than not either fabricated, or altered in whole or
in part, the evidence is admissible only if the proponent demonstrates that its
probative value outweighs its prejudicial effect on the party challenging the
evidence.

This proposal was considered to be unworkable as written and will be reworked before being reconsidered later.

Another proposal suggested subjecting machine-generated evidence to the same reliability requirements as expert witnesses

 concerns were expressed about hampering prosecutions (in criminal cases) by allowing defense lawyers to challenge any digital evidence without establishing a sound basis on which to question it.



### Can AI Affect Judges Themselves?

There are circumstances in which a Court or tribunal may seek or rely information not in evidence. In a judgment in patent litigation over motor oil additives, in which there were several expert witnesses called by the parties, the Judge in the Federal Court referred to a document not in evidence:

• "A Consumer Report for February 1987, with material obtained courtesy of the American Petroleum Institute, provides a splendid summary for the non-chemist consumer."

and quoted several passages from the document, including passages referring to the purpose of additives in motor oils.

According to the Court's reasons:

 "The above is incorporated more as an information piece for the uninformed or uninitiated. The chemists here - the expert witnesses - have provided a suitable glossary of terms also aimed at the uninformed/uninitiated which glossary is appended to these reasons as Appendix B."

The Court conducted its own research to supplement sworn evidence of experts who were subject to cross-examination on their views.



#### The Judge's Knowledge in Trademark Cases.

The Supreme Court of Canada in *Masterpiece Inc. v. Alavida Lifestyles Inc.* considered the role of experts and survey evidence in trademark litigation, and said:

• Generally, an expert should only be permitted to testify if the testimony is likely to be outside the experience and knowledge of the judge. Where the "casual consumer" is not particularly knowledgeable and there is a resemblance between the marks, expert evidence that simply assesses that resemblance will not usually be necessary. Judges should consider the marks at issue, each as a whole, but having regard to the dominant or most striking or unique feature of the trade-mark, using their own common sense, to determine whether the casual consumer would be likely to be confused when first encountering the trade-mark.

The Court criticized both the expert evidence in the case and some of the survey evidence adduced by the parties.



## **Expert Evidence was not Necessary**

"A significant part of the trial judgment, and argument ... was dedicated to the expert evidence .... This evidence took two forms: expert testimony adduced by Alavida on how a consumer is likely to react when presented with the trade-marks, and a survey conducted by an expert for Masterpiece Inc. which was heavily critiqued by an expert for Alavida.

"...[T]expert evidence on either side was not particularly helpful. Significant parts ... were contradictory and acrimonious. In the result, these disputes appear to have substantially distracted from the confusion analysis rather than assisting it."

The first problem, said the Court, was that much of the expert testimony was not "necessary".

 "[W]here the "casual consumer" is not expected to be particularly skilled or knowledgeable, and there is a resemblance between the marks, expert evidence which simply assesses that resemblance will not generally be necessary. And it will be positively unhelpful if the expert engages in an analysis that distracts from the hypothetical question of likelihood of confusion at the centre of the analysis."



#### The Role of Judges in TM cases

In Masterpiece, the SCC adopted the observations of Lord Diplock in *General Electric Co. v. The General Electric Co. Ltd.*, [1972] 2 All E.R. 507 (H.L.)., distinguishing between goods sold in a specialized market to sophisticated consumers, and those sold to the general public.

In a specialized market where the targeted consumers have special knowledge or sophistication, expert evidence may be essential to determining when confusion would be likely to arise.

However, where goods are sold to the general public for ordinary use:

• "... the question whether such buyers would be likely to be deceived or confused by the use of the trade mark is a 'jury question'. By that I mean that if the issue had now, as formerly, to be tried by a jury, who as members of the general public would themselves be potential buyers of the goods, they would be required not only to consider any evidence of other members of the public which had been adduced but also to use their own common sense and to consider whether they would themselves be likely to be deceived or confused.



## Judge plays the part of the Jury

The question, Lord Diplock said, is not answered differently when the issue is determined by a judge.

"The judge's approach to the question should be the same as that of a jury. He, too, would be a potential buyer of the goods. He should, of course, be alert to the danger of allowing his own idiosyncratic knowledge or temperament to influence his decision, but the whole of his training in the practice of the law should have accustomed him to this, and this should provide the safety which in the case of a jury is provided by their number. That in issues of this kind judges are entitled to give effect to their own opinions as to the likelihood of deception or confusion and, in doing so, are not confined to the evidence of witnesses called at the trial is well established by decisions of this House itself."

Is it safe to assume that a judge, considering a trademark case, and applying her own knowledge, experience and common sense to the question of confusion is immune from the effects of "fake news".



## Deep fake technology

Leverages machine learning algorithms to insert other images, faces and voices into real images, video and audio recordings

Enables the creation of realistic impersonations out of digital "whole cloth"

Shifts balance from easy detection of fakes by enabling creation of images, videos and audios that are more difficult to debunk

Training examples allow neural network, for example, to create increasingly accurate models

Those who attended ABC in Edinburgh may recall creation of a picture of a buffalo herd

Now, GANs (generative adversarial networks) interact to produce better images much more quickly

Generator network produces image; discriminator network assesses how well the generator has done and instructs the generator on what changes should be made.



#### Concerns about fake evidence

Falsified evidence finds its way into the record of the court or tribunal and causes an unjust result

Increased likelihood that the opposing party will challenge your evidence, even without any real basis for doing so.

Decision makers are more aware of the existence of deepfakes and may be more inclined to give weight or credence to arguments that evidence is "fake news".



## Kyle Rittenhouse homicide trial

During the November 2021 homicide trial of Kyle Rittenhouse, the prosecutor sought to show the jury footage on an iPad of the defendant fatally shooting Joseph Rosenbaum, and indicated he would use the pinch-to-zoom function on the iPad to present a larger image to the jury.

#### Rittenhouse's counsel objected:

- the iPad uses artificial intelligence and "logarithms" "to create what [the algorithms] believe is happening.
- Not enhanced video, but Apple's iPad programming creating what it thinks is there

#### Prosecutor:

- the zoom-in function was "industry standard" and the jury would understand it was routine
- the defence was trying to take advantage of [the 75 year old Judge's] lack of knowledge about technology.
- The defense should have to present expert testimony that the image was adulterated



# Kyle Rittenhouse trial, continued

The Judge sided with the defense:

- the prosecution had the burden of proving that the Apple iPad does not use artificial intelligence to manipulate footage,
- gave the prosecution a 15-minute recess to locate an expert to testify that the zoomed-in image was "in its virginal state."

The prosecution did not produce such a witness. Instead, showed the jury "the original, zoomed-out clips on a Windows machine hooked up to a large TV in the courtroom" that did not fill the entire screen.

The Judge looked at the images with a magnifying glass.



#### Jan 6 Defendants

One defendant refused to agree to the admission of YouTube videos of events of Jan 6 events

• "relying on open-sourced media with no evidence of a chain of custody should not meet" the low threshold for admitting this kind of evidence.

Prosecutors argued that YouTube videos could be authenticated by distinctive comparison points with police body cameras.

Another defendant refused to agree to the admission of messages, videos and photos that he had shared with his family and friends.

Defendant's counsel was asked by the Court if he had any good faith basis for the questions about alleged fakes, and responded that he wanted to ask questions to the FBI witness about possible alteration of the images, but did not.

The evidence was admitted.



## Cheerleader Jealousy

In early 2021, the mother of a member of a cheer-leading team sent to the team management videos of members of her daughter's cheerleading team in states of undress and drinking and vaping, in violation of team rules.

The accused members and their parents claims that the photos were fakes.

A Pennsylvania DA charged the mother with online harassment and alleged publicly that the defendant disseminated deepfake videos of other members of the team.

The police subsequently dropped the deepfake allegation, conceding that there was insufficient evidence to show that the videos were faked.

The DA subsequently conceded that he had no knowledge of technology and appears to have assumed that the images were fake because the girls in the videos would not have done things like that.

While the prosecutors abandoned the deepfake allegations prior to trial, this episode points to the dangers of litigants' claims about cutting-edge manipulation running ahead of the facts.



#### The Challenges of Deepfakes

In light of these examples, how should courts and litigants approach the challenges of Deepfakes ?

In the US, Federal Rules of Evidence set the standards for the authentication of multimedia evidence, and courts will apply them, or their analogs in other jurisdictions, when assessing questions around Al-manipulated media, such as deepfakes.

Rule 901 requires that the proponent of evidence show that such evidence is what it purports to be, and provides a nonexclusive list of ten examples of how this can be done, including by introducing testimony of a witness with knowledge that an item is what it is claimed to be and by using the distinctive characteristics of the evidence itself "taken together with all the circumstances."

Evidence, such as open-source video, can also be compared with "an authenticated specimen by an expert witness or the trier of fact."

Where litigants have genuine concern about the veracity of media, they can challenge admissibility under various rules of evidence on the basis that the evidence may have been faked.



#### Obligations of the Attorney

Codes of Conduct and Ethical Behaviour

For example, the American Bar Association's Model Rules of Professional Conduct are clear that an attorney may "not knowingly ... offer evidence that the lawyer knows to be false," like a deepfake.

If he or she comes to know that evidence offered by a client or witness is false, the lawyer "shall take reasonable remedial measures," including disclosing that fact to the court.

And an attorney "may refuse to offer evidence ... that the lawyer reasonably believes is false," such as a video he or she reasonably believes to be manipulated.

Nothing new in these obligations.



#### **Professional Conduct Obligations**

But the possibility that deepfake media may be submitted as unadulterated evidence does not give litigants carte blanche to baselessly question evidence.

According to the ABA's Criminal Justice Standards for the Defense Function, "[d]efense counsel should not make objections without a reasonable basis."

If litigants raise such questions without a good faith basis, they risk undermining "the public's understanding of and confidence in the rule of law and the justice system," in the words of the Model Rules of Professional Conduct.

Doing so may violate professional rules against making frivolous arguments, baselessly denying factual contentions, or engaging in harassing, delaying or costly motion practice.



#### **Balance Ethics with Advocacy**

At the same time, counsel must balance their ethical duties with zealous advocacy in challenging evidence when there is good reason to do so.

Your investigation of the merits of the case against your client should include a diligent evaluation of the prosecution's evidence

- possible re-testing or re-evaluation of physical, forensic, and expert evidence)
- consideration of inconsistencies, potential avenues of impeachment of prosecution witnesses,
- other possible conclusions and alternative theories that the evidence may raise.

As it is, litigants will need to contend with the mere publicized existence of deepfakes and the doubts that can arise in the minds of jurors, even without egging on by counsel.



#### **Best Practices**

#### Authentication of evidence

"[t]o make the certification more persuasive to the Court, it may be useful to point out other indicia of reliability in the certification."

For example, if a litigant wants to authenticate the contents of a website, the certification may point out the website's distinctive design, that contents on the webpage remain on the site for the court to verify, that the owner of the website has published the same contents elsewhere, and the period of time the information was posted on the site, among other things.

Increasingly common that that the only available copies of documents are from electronic storage. Federal Rule 902(14) authorizes a certification to authenticate a digital copy of data taken from a device or system, such as a mobile phone or hard drive.



#### Be Vigilant

Do not take any evidence for granted, even evidence from your own client.

Be prepared for challenges of what used to be relatively unassailable evidence.

Be able to address questions regarding the evidence's chain of custody.

Provide circumstantial evidence to help establish the authenticity of open-source imagery and video. Circumstantial evidence can provide context of where and when imagery or video was taken, how it originated and whom it depicts.

Prepare forensic witnesses to address questions around deepfakes.

Be knowledgeable about the technology you are using. In the Rittenhouse trial, prosecutors were caught flat-footed when defense counsel asserted that Al manipulated the pinch-and-zoom function on the prosecutor's iPad.

Do not tie your own credibility to the credibility of your client.



## Question the other party's evidence

Review disclosed evidence in advance of the trial.

Most common law courts require advance notice, disclosure and the opportunity to challenge records intended for use at trial. Parties should leverage these opportunities to review media evidence for possible manipulation.

If media is questionable, consider retaining an expert to explain why it may be inauthentic.

Have a good faith basis to question any evidence. Courts should require litigants to demonstrate a good faith basis for their questions about whether media evidence is a deepfake.



#### **Before Using Al**

#### Perform vendor due diligence

- Assess the generative AI vendor's experience, reputation, reliability, financial stability, and compliance with legal standards including data security and privacy laws
- Consider creating or utilizing a checklist or questionnaire to gather essential information during your evaluation process

Assess competency and establish guidelines

- Evaluate your knowledge and proficiency in using the AI tool as well as your understanding of its advantages and potential risks
- Establish guidelines for utilizing the AI tool, ensuring that you and your employees have the requisite skills and information to navigate the tool competently and ethically

Review the terms of service

- Thoroughly review the terms of service for the AI tool and identify potential conflicts with your professional obligations
- Understand the vendor's responsibilities in the case of data breaches, cyberattacks, or other risks of inadvertent disclosure



# Before Using AI (2)

#### Develop communication protocols

- Identify scenarios where transparent communication about AI tool usage with a client is required to manage expectations and mitigate risk. Specify instances in which informed client consent should be obtained
- •Establish clear and well-defined communication protocols for discussing AI usage with clients

Identify limits and capabilities

- Conduct thorough research and experiment with the AI tool to gain a comprehensive understanding of its capabilities and limitations
- Consider how easily the AI tool integrates with your existing systems or software



# Before Using AI (3)

#### Implement data safeguards

- Understand how the data you input into the AI tool is handled, stored, and protected
- Determine what security measures the vendor has in place to protect the AI tool from unauthorized access
- If necessary, establish additional protocols to protect confidential client information from inadvertent disclosure

#### Conduct testing and validation

- Determine how the AI tool was trained\* (e.g., ask the vendor for information regarding the source of the dataset, how the data was labelled and validated, and what algorithms were used to train the AI tool)
- Use this information to identify and mitigate data biases and other risks



## While Using Al

Incorporate a human verification process

- Integrate a system or process\* of human verification to review AI-generated results and ensure their accuracy and reliability
- Identify tasks or legal processes where human judgment is critical, and the AI tool should not be employed

Provide ongoing training and solicit feedback

- Offer continuous training to AI users to ensure they utilize the tool in a manner consistent with your legal and professional obligations
- •Gather regular feedback on the AI tool's performance, usability, and areas that require refinement or improvement



## While Using AI (2)

#### Maintain an audit trail

- Establish a systematic process for recording all prompts and inputs you or your employees provide to the AI tool
- Regularly review the audit trails to identify potential risks, anomalies, or other issuesand take proactive steps to mitigate same

Supervise AI usage by employees

- Educate AI users on appropriate prompts, including specifying which prompts to avoid. Emphasize the importance of maintaining confidentiality in all interactions with the AI tool
- Regularly monitor employee AI usage and consider implementing user permissions and access controls to limit input



## While Using AI (3)

Prioritize client confidentiality

- •Instruct AI users not to input prompts that could identify clients or specific legal matters
- Establish clear protocols for anonymizing or removing sensitive data used as prompts Avoid copyright infringement
- Ask the AI vendor about whether the tool was trained with any restricted copyrighted content and if so, review the terms of use relating to such content
- •Exercise your own judgement when dealing with AI-generated content and ensure you contribute your own expertise and insights to the outcome



## After Using Al

Evaluate performance and effectiveness

• Based on use, testing, and feedback, assess the impact of the AI tool on efficiency, accuracy, and productivity

Conduct audit and compliance checks

• Conduct periodic compliance, ethical, and security audits to identify and address any vulnerabilities and to ensure ongoing compliance with your legal and professional obligations

Document AI-generated outcomes

• Maintain a record of the outcomes generated by the AI tool making sure to record instances where the AI recommendations were hallucinations or based on false or fabricated data



## Always

Stay current on AI developments

• Keep up with the latest developments in AI to ensure compliance with evolving legal regulations, ethical responsibilities, guidelines, and standards





#### Douglas N Deeth

Managing Partner

+1 416 941 9442 ddeeth@dww.com

#### Deeth Williams Wall LLP

Lawyers, Patent & Trademark Agents

**DWW.com** 



# THIS SESSION IS POWERED BY BSKB



# Official Sponsor of FICPI in 2024 Claiming Tomorrow Today™





# FICPI // Events 2025





FICPI World Congress & ExCo Meeting 12-18 October 2025 Naples, Italy

FICPI Korean Symposium 2-5 April 2025 Jeju Island, Republic of Korea



Scan the QR to sign up for advance information and updates



