Strafford

Presenting a live 90-minute webinar with interactive Q&A

Evidentiary Challenges in Divorce Cases: From Writings and Photos to Text Messages and Social Media

Authenticating, Admitting, and Objecting to Admission of Evidence and Testimony

TUESDAY, MAY 3, 2022

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

David K. Wilkinson, CFLS, AAML, Co-founder, **Wilkinson & Finkbeiner, LLP**, San Diego, CA

Christina E. Djordjevich, Partner, **Walzer Melcher LLP**, Woodland Hills, CA

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 ext.1 or visit Strafford's website at www.straffordpub.com.

EVIDENTIARY CHALLENGES IN DIVORCE: AUTHENTICATING WRITINGS, ESI, TEXTS, SOCIAL MEDIA, WEBCAM VIDEO, AND LAY OPINIONS

Christina E. Djordjevich

David K. Wilkinson

PRESENTERS

Christina E. Djordjevich
Partner
Walzer Melcher LLP
ced@walzermelcher.com

David K. Wilkinson
Co-founder
Wilkinson & Finkbeiner, LLP
david@wf-lawyers.com

TYPES OF ELECTRONIC EVIDENCE

Email Accounts and Messages

Social Networking Accounts

Text Messages and Chat Room Content

Website Content and Postings

Digital Photographs

Computer Stored Records and Data

EVER-EXPANDING SOCIAL NETWORKING SITES

- Twitter
- Facebook
- Instagram
- TikTok
- Snapchat




THAT'S IT, RIGHT?

NOT EVEN CLOSE.

THERE ARE WELL OVER 500 SOCIAL MEDIA NETWORKING SITES.

QUICK NOTE ON PRIVACY

- Scrutinize any evidence you are seeking to potentially acquire / introduce from a privacy and legality perspective

PERSPECTIVES ON DIGITAL PRIVACY

- Perspective #1: "In this [social media] environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking." *Romano v. Steelcase*, 30 Misc. 3d 426, 434 (N.Y.S. 2010)
- Perspective #2: "That the people shall be secure in their…electronic communications and data…" Mo. Const., Art. I, § 15, enacted 2014.
- In criminal and tort law, the omnipresence of Big Brother is no excuse for violating another's privacy rights.

CIVIL AND CRIMINAL PENALTIES

- Tort for Invasion of Privacy – Reading private, password protected emails can implicate a civil claim for invasion of privacy in some states
  - See Restatement (Second) of Torts, § 652B
  - Video taping in the home, especially the bedroom, without the other spouse's knowledge can create civil liability. Example: *In re Marriage of Tigges*, 758 N.W.2d 824 (Iowa 2008).
- "Nothing in…common law suggests that the right of privacy is limited to unmarried individuals." Clayton v. Richards, 47 S.W.3d 149, 155 (Tex. Ct. App. 2001)

CIVIL AND CRIMINAL PENALTIES

- **Computer Fraud and Abuse Act** (18 U.S.C. § 1030) – Prohibits intentionally accessing a computer without authorization or exceeding authorized access
  - Up to 1 year imprisonment and a fine
  - Unless the court determines you committed a tortious act in doing so—then the penalty is up to 5 years imprisonment and a fine.
- *Mahoney v. Denuzzio*, 2014 U.S. Dist. LEXIS 10931 (D. Mass. 2014) (Ex-girlfriend obtained access of the former boyfriend's email and Facebook account, altered information in those accounts, and sent racist messages on multiple occasions)
- *United States v. Kernell*, 667 F.3d 746 (6th Cir. 2012) (college student found guilty under the CFAA for hacking into former Governor Palin's Yahoo! email account).

FEDERAL WIRETAP ACT APPLIES TO **MARRIED COUPLES**

- There is no "interspousal immunity" for wiretapping under the statute.
- Each spouse has an *individual expectation of privacy* in communications covered by eavesdropping and wiretapping laws that the marital relationship *does not preclude*.
- Not all courts agree on what a "reasonable expectation of privacy" is in a marriage – check the statutes/case law in your state.

DO NOT…

- Take possession of illegally obtained materials and evidence. Having it in your possession, reading it, and/or listening to it may be a **crime.**
- Represent an individual who has obtained electronic materials through illegal means.
- Attempt to introduce evidence which has been illegally obtained by a client or other party.

IPHONE APPLICATIONS TO BE AWARE OF

Voice Memo - Turns your phone into an audio recording device.

- **<u>WARNING:</u>** Exercise extreme caution when secretly recording conversations. Some states require two-party consent.

Find My Friends - Allows you to share your location or view other people's location.

Find My iPhone - Allows remote location-tracking of iPhones, iPads, and Mac computers.

Remember to change all passwords and login information!

ANDROID AND BROWSER APPS

- SMS to Text
- SMSBackup+
- Android Device Manager – locate and erase your Android device

SOCIAL NETWORKING SITES HAVE A SUBSTANTIAL IMPACT IN FAMILY LAW PRACTICE

- Social media sites are both a source of information and a cause for concern
- Social media can play a large role in divorce cases, particularly with respect to custody
- Advise clients to be cognizant about what they post

SOCIAL MEDIA IN FAMILY LAW PROCEEDINGS

- Suspicion of abuse, compromising photos, inappropriate activity that shows up on Facebook, are all fair game.
  - Example: Elissa N. v. Ian B., 32 Misc 3d 1215(A); 930 NYS2d 174 (Fam Ct) (April 7, 2011).
  - Mother used Facebook and blogs to rant about ex-husband.; impacted Court's decision that mother was a less fit parent than the father
- Lawyer should not use **trickery,** such as friending a person under false pretenses to gain access to private information.
  - Example: Philadelphia Op. 2009-02; Assoc. of the Bar of New York, Op. 2010-2.

HOW TO OBTAIN SOCIAL MEDIA EVIDENCE

- Direct access to Responding Party's account by the Requesting Party (or attorney or special master)
  - Intrusive and concern of manipulation
  - *Largent v. Reed*, No. 2009-1823 (Pa.C.C.P. Nov. 8, 2011) – Court ordered party to turn over Facebook login information; designated lawyer as only party who could access for a limited time
- Discovery to Responding Party
- Subpoena
  - Worth the time?
  - Facebook: Stored Comm. Act (SCA) prohibits disclosure
  - Domesticate in CA

EXAMPLES OF SOCIAL MEDIA ESI

Facebook:

- Can download account information.
- Users can download a zip file containing timeline information, posts, messages, photos, ads that the user clicked and even the IP addresses that are logged when the user accessed their Facebook account.

Twitter:

- Offers similar option to download account information but on a more limited basis.
- Users can request the user's archive which will provide a history of the user's tweets.
- Users must request this information directly by sending an e-mail to privacy@twitter.com with the subject line, "Request for Own Account Information."

EXAMPLES OF SOCIAL MEDIA ESI

TikTok:

- Includes three main categories of downloadable data: "Your Profile", "Your Activity" and "Your App Settings."
- Can request this data in the App and it will be downloaded to your phone.

Snap Chat:

- Despite time limiting features, there are still ways of accessing a user's history.
- App retains significant amount of data, including who you have chatted with, searched for, filters used, and login location
- Must request the data download in settings and company will email a link to access the history.

ELECTRONIC COMMUNICATION PLATFORMS

- Text Messages
  - Cell providers retain information relating to sending / receiving texts, but not substance of texts
- Email – Gmail, Yahoo!, etc.
- Instant messaging services, etc. - i.e., WhatsApp, Skype, Google Hangouts, Viber, Facebook Messenger, iMessage, LinkedIn, Snapchat, Microsoft Teams
  - Retention depends on provider (e.g., Snapchat automatically deletes)
  - Mostly cloud-based, enabled on multiple devices

THE "DARK" WEB AND "DEEP" WEB

- Deep Web:
  - Includes private servers not accessible to public (i.e. a chess club)
  - Anything behind a paywall or that requires user credentials to access
  - Almost entire internet is Deep Web (more than 90%)
- Dark Web:
  - Part of internet that is not indexed by search engines
  - Intentionally hidden and requires specific browser
  - Lots of criminal activity (buy credit card numbers, guns, drugs, etc.)
- A website that is taken down is still out there!

PRESERVATION OF EVIDENCE, INCLUDING ESI

- Notice to client to preserve data
  - *Lester v. Allied Concrete Co.*, No. CL08-150 (Va. Cir. Ct. Sept. 1, 2011 – Court sanctioned both party and counsel for failing to preserve social media content
  - Lawyer advised client, through paralegal, to "clean up" his Facebook page.
- Notice to opposing party / counsel
- Email David for templates: david@wf-lawyers.com
- Spoliation
- Resources
  - Cloud Preservation and X1 Social Discovery – specifically designed to collect and archive social media content

EVIDENTIARY CONSIDERATIONS FOR ELECTRONICALLY STORED INFORMATION EVIDENCE (ESI)

- Certain evidentiary impediments must be overcome, particularly the Federal Rules of Evidence (FRE).
- Regarding ESI, "no additional authentication is required just because the records are in computerized form rather than pen and pencil."
- Attorneys should address the **accuracy** and **reliability** of computerized evidence to ensure it is not challenged for the first time at trial.

FEDERAL RULES OF EVIDENCE

FRE 104: Preliminary Questions

Under Rule 104, the court has to determine whether a foundation for authenticity exists.

Example:

- If an email is offered into evidence, determination of whether it is authentic rests with the jury under 104(b), and the facts under consideration would be admissible into evidence.

FRE 401: Relevance

Evidence must be **relevant** under FRE 401.

- This basically means whether evidence would tend to make the existence of a fact *more or less probable* based on its admission.
- This is generally a lower hurdle to overcome.

FEDERAL RULES OF EVIDENCE:

FRE 901 AUTHENTICITY

- Authentic evidence is "a finding that the matter in question is what its proponent claims."
- Counsel must have a **prima facie** showing of authenticity.
- Attorneys **regularly fail** to address this requirement.
- Evidence can be authenticated through extrinsic evidence such as:
  - Testimony of witness with knowledge
  - Comparing emails previously authenticated with evidence in question
  - Public records
  - Circumstantial evidence
    - The content of what an email says can often authenticate it. *United States v. Siddiqui,* F.3d 1318 (11th Cir. 2000).
    - Can also be proven through certain types of metadata.
- In *United States v. Safavian* (D.D.C. 2006), the court held:
  - "The question for the court under Rule 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is.'"
  - This requires attorneys to find the necessary evidence to establish the facts and identify corroborating witnesses.

FEDERAL RULES OF EVIDENCE

FRE 902: Self-Authenticating

- Authentication can be achieved **without extrinsic evidence**.
- There are **12** methods of self-authentication listed
- Examples of methods that have been used in courts to authenticate ESI:
  - **Official Publications** – *Equal Opportunity Commission v. E.I. Dupont De Nemours and Co.,* 2004 U.S. Dist. LEXIS 20748 (E.D. La. 20748).
  - **Self-Authentication by inscriptions, signs, tags, or labels** – *Lorraine v. Markel American Insurance Co.,* 2007 U.S. Dist. (D. Md. May 4, 2007).

FRE 801: Hearsay

- Evidence is Hearsay if it constitutes a statement offered for its substantive truth and is not excluded from the definition of hearsay. See *United States v. Rollins*

ORIGINAL WRITING RULE

- Also known as the "Best Evidence" Rule
- To prove the contents of a writing (or mechanical, electronic, or other familiar duplicate such as a photograph), a party must produce the original or, if unavailable, secondary evidence from testimony of the drafter or a person who read the document

FEDERAL RULES OF EVIDENCE 1001 – 1004

- FRE 1001 defines "original" of a writing or recording as the "writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout--or other output readable by sight--if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it.
- FRE 1001 defines "duplicate" as "a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original."

FEDERAL RULES OF EVIDENCE 1001 – 1004

- FRE 1002 requires an original writing, recording, or photograph in order to prove its content unless these rules or a federal statute provides otherwise.
- FRE 1003 provides that a duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate.

FEDERAL RULES OF EVIDENCE 1001 – 1004

- FRE 1004 states that an original is not required and other evidence of the content of a writing, recording, or photograph is admissible if:

  (a) all the originals are lost or destroyed, and not by the proponent acting in bad faith;

  (b) an original cannot be obtained by any available judicial process;

  (c) the party against whom the original would be offered had control of the original; was at that time put on notice, by pleadings or otherwise, that the original would be a subject of proof at the trial or hearing; and fails to produce it at the trial or hearing; or

  (d) the writing, recording, or photograph is not closely related to a controlling issue.

SIX BASIC ISSUES OF ELECTRONIC EVIDENCE

#1 Proper authentication needed due to the possibility of alteration, or that the communication was manufactured

#2 Establish relevance

#3 Show that the posting, photo or other information was done by the person or entity who you claim it was posted by

#4 Has the person or entity shared the password with any other person or entity?

#5 Show that the person or entity profile contains identifiable personal information, including birthdates, photographs and other unique or known information

#6 Interrogatories should be issued to determine what sites a party uses, the IP address, usernames and passwords

LORRAINE V. MARKEL AMERICAN INSURANCE CO., 2007 U.S. DIST. (D. MD. MAY 4, 2007)

- Leading case discussing admissibility of ESI.
- Facts: Involved an insurance dispute over the recovery of insurance proceeds after Plaintiff's boat was struck by lightning.
- Introduced Five Hurdles to Introducing Electronically Stored Information:
  1) Relevance
  2) Authentication
  3) Hearsay
  4) Original Writing Rule
  5) FRE 403: Balancing

AUTHENTICATION OF TEXT MESSAGES AND EMAILS

Who sent the message?

What is the date and time of the message?

Who is the recipient of the message?

Be sure to provide an accurate and complete reproduction of the message.

AUTHENTICATION OF SOCIAL MEDIA POSTS

Does the representation of the post fairly and accurately depict how the post appeared online at the time?

Does the post actually relate to a person or issue involved in the case?

If the content includes a statement, can the content be attributed to the purported maker?

IN THE INTEREST OF A.D.W., 821 N.W.2D 778 (IOWA CT. APP. 2012)

- In case involving termination of mother's parental rights, the court held that the trial court should ***not*** have allowed into evidence a picture from the mother's Facebook depicting a marijuana-growing operation.
- Admitting the picture was inappropriate due to lack of proper authentication.
- Witness had no personal knowledge re whose marijuana operation was depicted, who took the photos, who posted it on Facebook, or whether the mother was aware that the photo appeared on her Facebook page.

TIPS FOR ADMITTING EVIDENCE

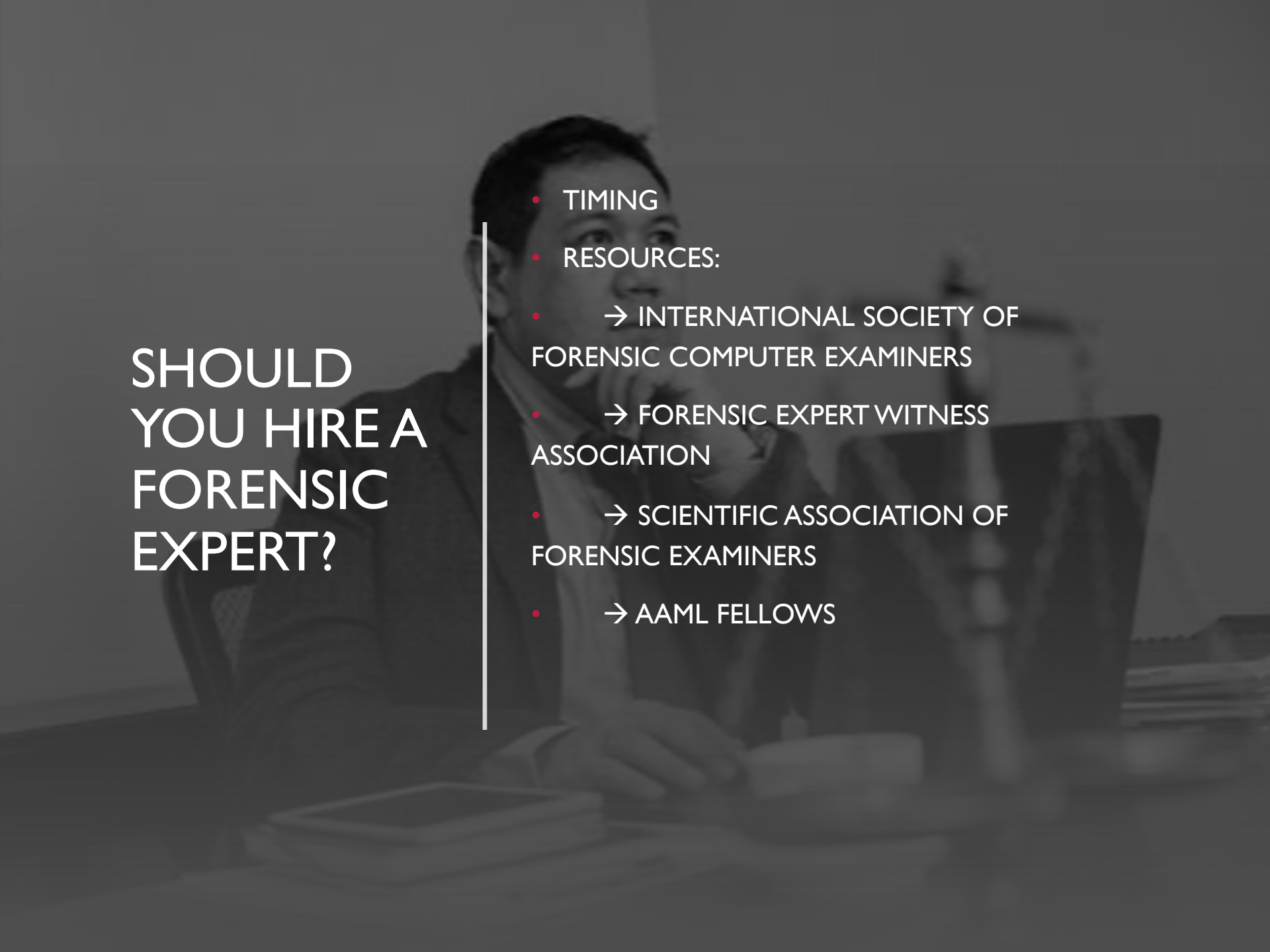
- Authentication through admissions of opposing party
- Authentication by compelling circumstantial evidence possible
- Eliminates problems with third party providers
- The basic rules don't change with electronic evidence, but important to know the media itself, protocols, and standards for admissibility

WATCH OUT FOR MANIPULATED ESI:

- Subpoena source documents
- Use available tools
  - Facebook → Go to "Settings" and view list of all devices used to log in and their location
  - Twitter → Go to "Settings" and view all data
  - Google → Go to "Device Activity" to view which devices are signed in
  - Instagram → Go to "Settings" to view third party services
  - Run anti-virus software
- Phishing

WATCH OUT FOR MANIPULATED ESI

- Pay attention:
  - Has a signature been forged?
  - Has an electronic document been altered?
  - Has text been cut and pasted, or altered?
  - Has an image changed?
- When in doubt, consult a forensic expert!
- Deal with manipulated data as early as possible



SHOULD YOU HIRE A FORENSIC EXPERT?

- TIMING
- RESOURCES:
- → INTERNATIONAL SOCIETY OF FORENSIC COMPUTER EXAMINERS
- → FORENSIC EXPERT WITNESS ASSOCIATION
- → SCIENTIFIC ASSOCIATION OF FORENSIC EXAMINERS
- → AAML FELLOWS

LAY WITNESSES AND OPINION TESTIMONY

- Lay witness offering opinion on whether a document has been manipulated or not?
- Lay witness offering opinion on authenticity of an electronic communication?
- Lay witness offering opinion re handwriting identification?
- Lay witness offering opinions on other issues?

LAY WITNESSES AND OPINION TESTIMONY

- A lay witness is any witness who is not testifying as an expert witness.
- Testimony of lay witnesses must be based on perception or personal knowledge
- Contrast with expert witness, who may provide opinion based on expert's scientific, technical or other specialized knowledge. **See FRE 702**.

LAY WITNESSES AND OPINION TESTIMONY

- Lay witnesses may offer opinion testimony where opinion is: "(a)rationally based on the witness's perception; (b) helpful to clearly understand the witness's testimony or to determining a fact in issue; and (c) not based on scientific, technical, or other specialized knowledge." **FRE 701.**
- Ask: is this lay witness's opinion based on the witness's perception, and what facts or information did this lay witness rely on in forming the opinion? Does the opinion require scientific, technical, or other specialized knowledge?

THANK YOU FOR ATTENDING!

If you have any questions, please email us:

ced@walzermelcher.com

David@wf-lawyers.com