



Capturing Webpages as Evidence: The Risks and Best Practices You Need to Know

ISBA: Civil Practice Update: Review on E-Discovery
May 19, 2016

Presenter: Patrick Schweih



Patrick Schweih

- Licensed Attorney in Illinois
- Expertise in anti-counterfeiting and webpage collection
- Selected member of INTA Internet committee
- Page Vault VP of Customer Solutions
- Serving Am Law 100, small/med, and solo

Agenda - Capturing Webpages as Evidence

1. The Growing Importance of Web Evidence (2 min)
2. Authenticating Web Evidence Under the Federal Rules of Evidence 901 (6 min)
3. Risks and Concerns (5 min)
4. Capture Methods (4 min)
5. Best Practices (8 min)



I. The Growing Importance of Web Evidence

Web Evidence Is Commonplace

- Electronically Stored Information (ESI) is everywhere, including web content
- Web now critical source of evidence



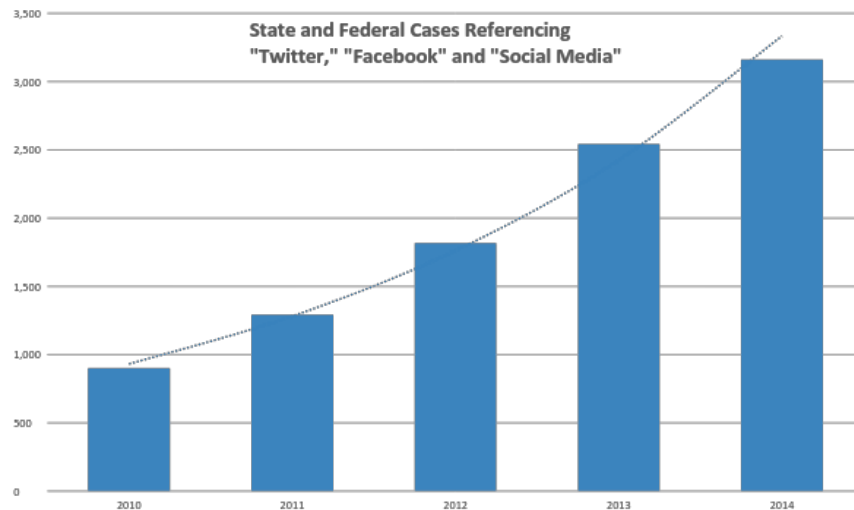
Web Evidence in Variety of Practices



CLASS ACTION



Trend is Clear – Web Evidence Growing



Source: Westlaw Search Terms "Facebook," "Twitter" and "Social Media" Referenced in State and Federal Cases from 2010-2014 (June 10, 2015).

II. Authenticating Web Evidence Under the Federal Rules of Evidence (FRE) and Illinois Rules of Evidence (IRE) 901

Authentication Standard: FRE 901(a) and the IRE 901(a)

- **FRE 901(a) – The Standard of Authentication**
 “[T]he proponent must produce *evidence sufficient to support a finding that the item is what the proponent claims.*”
- **IRE 901(a) – State Equivalent to FRE 901(a)**
 “The requirement of authentication or identification as a condition precedent to admissibility is satisfied by *evidence sufficient to support a finding that the matter in question is what its proponent claims.*”

How to Meet the Authentication Standard: FRE 901(b) and IRE 901(b)

FRE 901(b) and IRE 901(b) – Examples

- Non-exhaustive list of evidence that satisfies authentication requirement



Authenticating Web Evidence Under FRE 901(b) and IRE 901(b): 4 Common Ways

<u>Federal Rules of Evidence (FRE)</u>	<u>Illinois Rules of Evidence (IRE)</u>
FRE 901(b)(1): Testimony of a Witness with Knowledge	IRE 901(b)(1): Testimony of Witness With Knowledge
FRE 901(b)(3): Comparison by an Expert Witness or the Trier of Fact	IRE 901(b)(3): Distinctive Characteristics and the Like
FRE 901(b)(4): Distinctive Characteristics and the Like	IRE 901(b)(4): Distinctive Characteristics and the Like
FRE 901(b)(9): Evidence About a Process or System	IRE 901(b)(9): Process of System

FRE 901(b)(1) and IRE 901(b)(1): Testimony of a Witness with Knowledge

- Witness with “personal knowledge” of content can authenticate
 - Author, owner or creator of website
 - Viewer and capturer of the content (becoming problematic)

CHALLENGES:

1. Courts concerned about altering content especially when lacking metadata
2. Lack of knowledge if not the owner/creator
3. Attorneys don't want to involve their staff



FRE 901(b)(3): Comparison by an Expert Witness or the Trier of Fact

- A computer forensic **expert** can authenticate the webpage
 - Serves as a trusted third party
- Comparison by expert of authenticated webpage with proffered item
 - Most frequently used for authenticating handwriting or other hard-copy documents, but also applies to web

CHALLENGES:

1. Costly: money and time
2. Content disappears before capture



FRE 901(b)(4) and IRE 901(b)(4): Distinctive Characteristics and the Like

- Authenticate by evidence of distinctive characteristics and circumstantial evidence
 - Unique language, speech patterns, username
 - Metadata (time, date, url, hash values, etc.)

CHALLENGES:

1. Easy to create fictitious websites/social media accounts with distinctive characteristics
2. Likely requires supporting forensic evidence (URL, time, date)



FRE 901(b)(9) and IRE 901(b)(9): Evidence About a Process or System

- Authenticate through proof that capture was produced by a **process or system** that can produce a reliable result
 - Witness with “scientific, technical, or other specialized knowledge” (FRE 702, IRE 702) to explain system’s reliability and accuracy

CHALLENGES:

- Many capture tools are not designed for legal use (chain of custody, metadata)
- Need individual with specialized knowledge



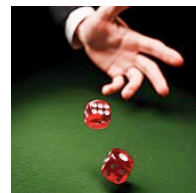
Authenticating Web Evidence Under FRE 901(b) and IRE 901(b): 4 Common Ways

<u>Federal Rules of Evidence (FRE)</u>	<u>Illinois Rules of Evidence (IRE)</u>
FRE 901(b)(1): Testimony of a Witness with Knowledge	IRE 901(b)(1): Testimony of Witness With Knowledge
FRE 901(b)(3): Comparison by an Expert Witness or the Trier of Fact	IRE 901(b)(3): Distinctive Characteristics and the Like
FRE 901(b)(4): Distinctive Characteristics and the Like	IRE 901(b)(4): Distinctive Characteristics and the Like
FRE 901(b)(9): Evidence About a Process or System	IRE 901(b)(9): Process of System

III. Risks and Concerns

Risk: Inconsistent Approaches

- Inconsistent approaches to authenticating web evidence across jurisdictions and judges
- Simple screen shots now being rejected
- Concern about ease of altering digital content
- Case law suggests lawyers roll the dice when merely presenting a print screen



Risk: Inaccurate Output With Standard Printout

- What comes out of printer doesn't look like the webpage
- Risk of confusion

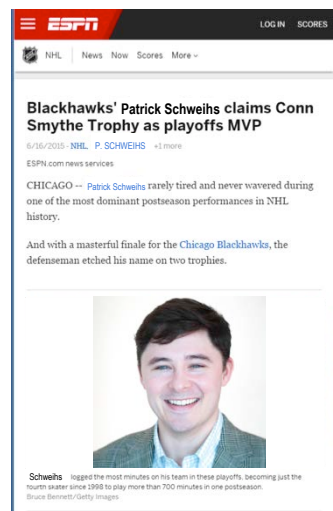
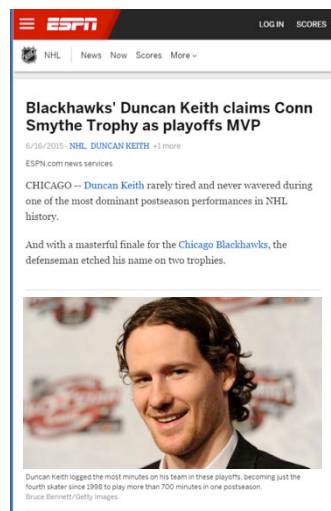


You want to print this...



...but printouts are misconfigured and missing content.

Tampering Example (very easy to modify digital images and content)



Risk: Insufficient Supporting Data

- Insufficient supporting evidence (such as metadata)
- Simple screenshot alone often not enough
- Metadata (“data about data”)



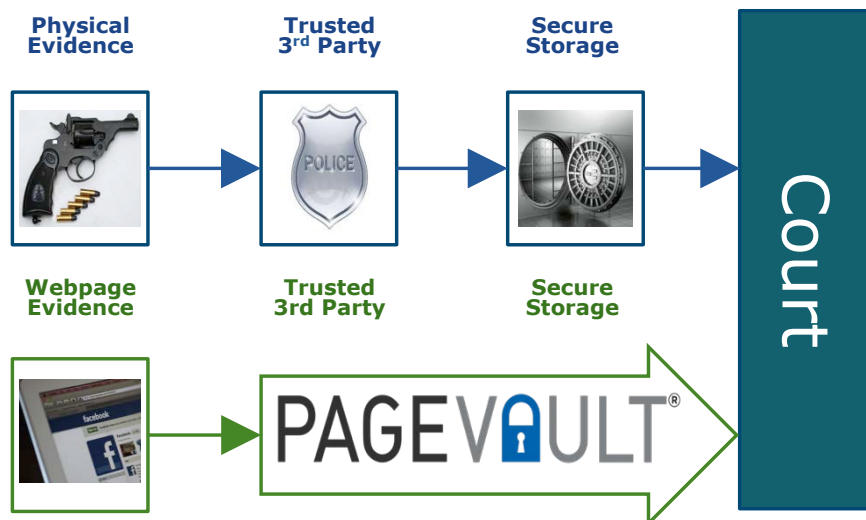
Document title:	Bill Gates Facebook
Capture URL:	https://www.facebook.com/BillGates
Captured site IP:	173.252.112.23
Page loaded at (UTC):	Wednesday, Jul 22 2015, 12:23:49
Capture timestamp (UTC):	Wednesday, Jul 22 2015, 12:24:27
Capture tool:	v3.0.6
Page Vault server IP:	54.175.100.67
Browser engine:	Chrome/41.0.2272.16
Operating system:	Microsoft Windows NT 6.2.9200.0 (6.2.9200.0)
PDF length:	36
Portal URL:	https://portal.page-vault.com/##/snapshot/8246
User:	testuser

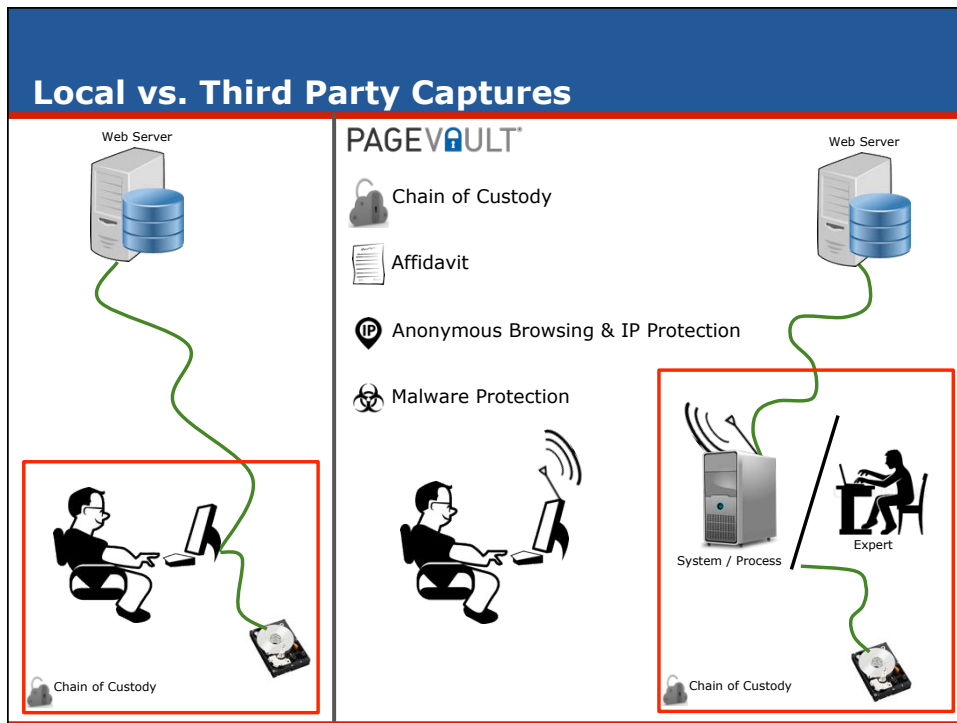
Risk: Ephemeral Nature of Web

- Content can be quickly changed or removed
- Websites updated in the standard course of business



Admissibility Risk & Chain of Custody





IV. Capture Methods

Capture Methods

1. Standard Printout/Print Screen/Save to PDF
2. Screen Capture Software
3. Forensic Software
4. Forensic Expert
5. Subpoenas

Method: Standard Printout/Print Screen/Save to PDF

PROS

- Simple
- Do-it-yourself



CONS

- User is in the chain of custody
- Manual recording of metadata
- Time-consuming for long pages
- Poor output (missing content)

Method: Screen Capture Software

PROS

- Easy to use
- Captures entire webpage



CONS

- Not built for legal use
- User is in the chain of custody
- Limited metadata (basic)
- Capture may not look exactly like the webpage

Method: Forensic Software

PROS

- Designed for legal use
- Captures entire webpage
- Automatically captures metadata and source files



CONS

- Complex/difficult to use – designed for IT professionals
- High training costs
- User may be in the chain of custody

Method: Forensic Experts

PROS

- Years of expertise
- Variety of tools at their disposal
- Trusted third party



CONS

- Expensive and time consuming
- Response time can be slow – online content can change or disappear

Method: Subpoena

PROS

- Access to content that is no longer publically available
- If produced, authentication isn't usually a hurdle

CONS

- Time consuming and litigious
- Private content protected by the Stored Communications Act (SCA) - Civil Subpoena won't work
- Digital records may be deleted

Note: Subpoenas to websites mostly fall under Stored Communications Act, 18 U.S.C. § 2701



V. Best Practices

Best Practices

1. Use Rigorous Standard
2. Use a Trusted Third Party
3. Use Secure Storage
4. Capture Metadata
5. Capture Source Files
6. Capture Webpages Immediately
7. Consider Spoliation
8. Uphold Social Media Ethics

Best Practice: Use Rigorous Standard

- Court's approach is inconsistent – from lenient to demanding - case law is unclear
- Recent decisions rejecting mere printouts
- Prepare for strict standard



Best Practice: Use a Trusted Third Party

- Trusted third party removes you from chain of custody
 - Forensic expert
 - Software solution designed for use with FRE 901(b)(9)



Best Practice: Use Secure Storage

- Digital
 - Hashing and digital signing of captured content
 - Secure, encrypted storage
- Physical/Printouts
 - Maintain control



Best Practice: Capture Metadata

- Collect metadata : time, date, URL, IP address, capturer, software version
- Automate capture of the metadata if possible
- More is better



Best Practice: Capture Source Files

- Collect source files: HTML & DOM
- Contains information not visible on the webpage



Best Practice: Capture Webpages Immediately

- Internet content changes by the moment
- Capture before it is removed, modified or access restricted



Best Practice: Consider Spoliation

- Capture your client's content as insurance against spoliation claims
- Capture opposing party's content in case of future spoliation
- Inform your client about their **duty to preserve evidence**
 - Instruct your client **not** to delete content



Best Practice: Uphold Social Media Ethics

- Do not create fake accounts to "friend"
 - Avoid communications with represented parties
 - Caution with unrepresented third parties
- Can create accounts to browse publicly available content



State Ethics Rules on Social Media: Friending

- **California (San Diego County Bar Association Opinion 2011-2)**
 - A lawyer could not send a Facebook friend request to gain access to their Facebook content
- **Oregon, Kentucky and New York**
 - Concluded lawyers are not permitted (either themselves or through agents) to engage in false or deceptive tactics to circumvent social media users' privacy settings to reach non-public information
 - Oregon (Op. 2013-189), Kentucky (Op. KBA E-434), New York State (Op. 843) and New York City (Op. 2010-2)
- **Philadelphia (Op. 2009-02)**
 - One step further concluding that lawyers must affirmatively disclose their reasons for communicating with the third party.

Questions?



Appendices

Appendix A: Case Law – Authenticating Web Evidence Under FRE 901(b)(1)

Appendix B: Case Law – Authenticating Web Evidence Under FRE 901(b)(3)

Appendix C: Case Law – Authenticating Web Evidence Under FRE 901(b)(4)

Appendix D: Case Law – Authenticating Web Evidence Under FRE 901(b)(9)

Appendix E: Case Law – Testimony of Person Capturing Third-Party Webpage Insufficient to Authenticate

Appendix A: Case Law – Authenticating Web Evidence Under FRE 901(b)(1)

***Standard Innovation v. Lelo, Inc.*, Case IPR2014-00148, slip op. 10 (PTAB April 23, 2015) (Paper 41)**

Printouts of webpages from the Internet Archive’s “Wayback Machine” inadmissible under FRE 901(b)(1) where proponent **did “not [provide] testimony of any witness with personal knowledge** of the information on the website or the associated printouts.”

***People v. Lenihan*, 911 N.Y.S.2d 588 (N.Y.Sup.Ct.2010)**

The court precluded defendant from cross-examining the People’s witnesses about their gang affiliation and confronting them with photographs defendant’s mother had printed from MySpace. These photos allegedly showed the witnesses making hand gestures and wearing clothing affiliated with a gang. The court held that defendant could not authenticate the photographs “[i]n light of the ability to ‘photoshop,’ [and] edit photographs on the computer.”

Appendix A (Cont.): Case Law – Authenticating Web Evidence Under FRE 901(b)(1)

St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 2006 U.S. Dist. LEXIS 28873 (M.D. Fla. May 12, 2006) *quoting In re Homestore.com, Inc. Sec.Litig.*, 347 F.Supp.2d 769, 782 (C.D. Cal. 2004)

The Court held that to authenticate printouts from a website, the proponent of the evidence must produce "some statement or affidavit from someone with knowledge [of the website] . . . for example [a] web master or someone else with personal knowledge would be sufficient."

Appendix B: Case Law – Authenticating Web Evidence Under FRE 901(b)(3)

People v. Beckley, 185 Cal. App. 4th 509 (Cal. Ct. App. 2010)

On appeal, the court held that the prosecution's failure to authenticate a photo downloaded from appellant's MySpace account should have barred its admission where:

- (1) the **proponent could not testify** from his personal knowledge that the photograph truthfully portrayed appellant flashing a gang sign (FRE 901 (b)(1));
- (2) "**no expert** testified that the picture was not a 'composite' or 'faked' photograph" (FRE 901(b)(3); and
- (3) "**digital photographs can be changed** to produce false images."

Appendix C: Case Law – Authenticating Web Evidence Under FRE 901(b)(4)

Smith v. State, 136 So.3d 424, 433-34 (Miss.2014)

The court held that the name and photograph on a Facebook printout were insufficient to link the communication to the purported author under Miss. R. Evid. 901(b)(4) (modeled after FRE 901(b)(4)). The court noted “[t]he ease with which defendants and alleged victims alike could **fabricate a social media account** to corroborate a story.”

Griffin v. State, 19 A.3d 415, 424 (Md.2011)

The court held that the witness's birthday, location, photograph and nickname listed on her alleged MySpace profile did not provide a foundation to authenticate the profile. The court reasoned that information generally known by a witness's friends and associates is **not sufficient "distinctive characteristics"** to authenticate a profile page. In addition, the court emphasized that someone other than alleged author could have created the site and posted the comment at issue.

Appendix D: Case Law – Authenticating Web Evidence Under FRE 901(b)(9)

St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 2006 U.S. Dist. LEXIS 28873, *5-6 (M.D. Fla. May 12, 2006)

Facts: Plaintiff tried to authenticate printouts of archived electronic documents retrieved from the Internet Archive to show what defendant's website looked like in 2000. To authenticate the printouts, plaintiff submitted affidavits of two fact witnesses who testified that the printouts correctly portrayed the webpage as it looked in 2000. Plaintiff also presented an affidavit from the Internet Archive's administrative director from a previous litigation

Holding: The court held that plaintiff did not meet the requirements for authentication. The court concluded that to satisfy the requirement of FRE 901, **plaintiff must provide a statement or affidavit from an Internet Archive representative with *personal knowledge*** of the contents of the Internet Archive website verifying the printouts are true and accurate copies of Internet Archive's records

Appendix D (Cont.): Case Law – Authenticating Web Evidence Under FRE 901(b)(9)

***Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 549 (D. Md. 2007) (emphasis added)**

Discussing the various ways to authenticate webpage evidence under FRE 901(b), the court emphasized that “[Rule 901(b)(9)] recognizes one method of authentication that is ***particularly useful in authenticating electronic evidence stored in or generated by computers.***”

***In re Vinhnee*, 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005) (emphasis added)**

Exploring the methods to authenticate webpage evidence, the court highlighted that “[t]he advisory committee note makes plain that ***Rule 901(b)(9) was designed to encompass computer-generated evidence...***”

Appendix E: Case Law – Testimony of Person Capturing 3rd-Party Webpage Insufficient to Authenticate

***Linscheid v. Natus Medical Inc.*, No. 3:12-cv-76-TCB, 2015 WL 1470122 (N.D. Ga. Mar. 30, 2015)**

The court held that a printout of a LinkedIn profile page was **not properly authenticated** by the declaration from the individual who merely printed the webpage.

***United States v. Vayner*, 769 F.3d 125, 131 (2d Cir. N.Y. 2014)**

The court concluded that there was insufficient evidence to authenticate a social media page where the government did not provide a sufficient basis to conclude that the proffered printout was defendant’s profile page.