



PROGRAM MATERIALS

Program #2971

April 15, 2019

The Role of Social Media in E- Discovery: Current Developments for All Attorneys

**Copyright ©2019 by Theresa M. Coughlin, Esq. and
Kristen A. Lejnieks, Esq., Jones Day. All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

SOCIAL MEDIA AND E-DISCOVERY: CURRENT DEVELOPMENTS FOR ATTORNEYS

Presented by Kristen Lejnieks & Theresa Coughlin
April 15, 2019





TOPICS

- Why Are We Here?
- Information Governance
- Identifying and Preserving Social Media
- Collecting Social Media Information
- Review & Production
- Rule 26 – Relevance and Proportionality Considerations
- Using Social Media as Evidence

**WHY ARE WE
HERE?**



SCOPE

- Traditional social networks only a small part of modern social media
- “Social Media” encompasses:
 - Networks (Facebook, LinkedIn)
 - Blogging platforms (Twitter, Reddit)
 - Voice and text messaging services (Skype, Viber, WhatsApp, Telegram)
 - Photo and video sharing networks (Instagram, YouTube, Pinterest, Snapchat)
 - Live-Streaming Video (Facebook Live and Periscope)



RECENT GROWTH

- As of January 2018, 69% of U.S. adults used social media
- 6 social media platforms have over 1 billion users
- Proliferation of mobile devices (4.68 billion worldwide)
- International growth
 - WeChat social network has more than 1 billion active monthly users in China and QQ over 802 million monthly active users in China
 - Viber, WhatsApp, Skype offer “free” international calling and messaging

CORPORATE USE



Fortune 500 companies

- 98% have corporate LinkedIn accounts
- 91% have corporate Twitter accounts
- 89% have corporate Facebook pages
- 75% have corporate YouTube accounts
- 63% have corporate Instagram accounts
- 53% have corporate blogs

IN LITIGATION

- Increasingly important in many legal areas
 - Complex Business & Tort Litigation
 - Labor & Employment Law
 - Family Law
 - Trademark & Copyright
 - Internal White Collar Investigations
- Growing corporate reliance on social media will only expand its relevance



IT'S DISCOVERABLE

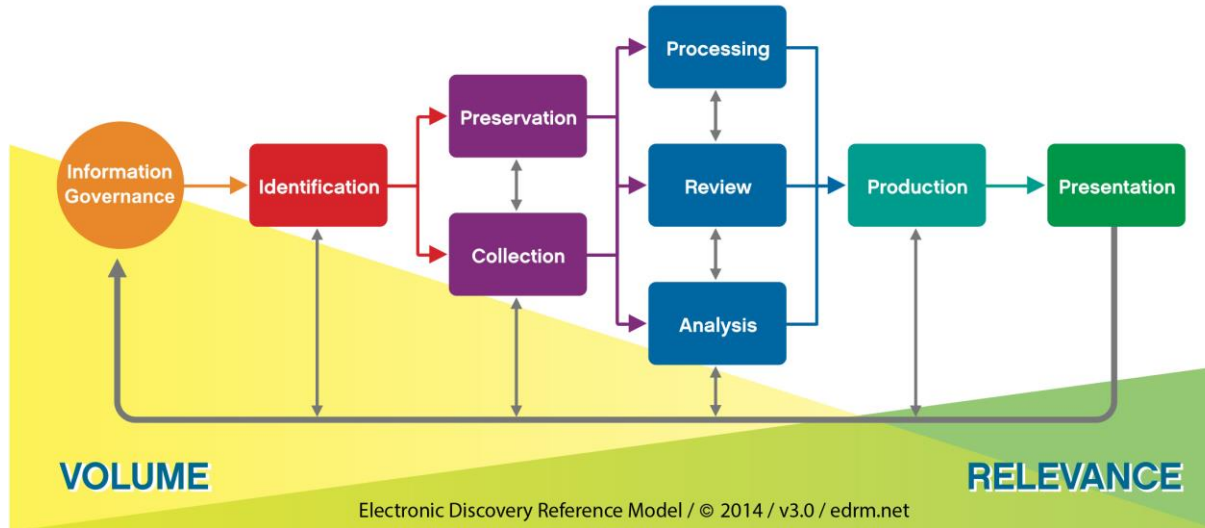
- Social media can qualify as a discoverable document under FRCP 34
 - “It is settled that information on social media accounts, including Facebook, is discoverable.” *Moore v. Wayne Smith Trucking Inc.*, 2015 WL 6438913 (E.D. La. Oct. 22, 2015); see also *In re White Tail Oilfield Services, LLC*, 2012 WL 4857777 at *2–3 (E .D.La. Oct. 11, 2012)
- Courts generally treat social media like any other ESI

LAWYERS' OBLIGATION TO LEARN THESE ISSUES

- Lawyers should familiarize themselves with e-discovery issues related to social media to provide competent representation (Model Rules and state bar association rules)
 - *Calvert v. Red Robin Int'l*, 2012 WL 1668980 (N.D. Cal. May 11, 2012) (holding lawyer can't use ignorance of social media as defense for not producing relevant discovery materials)
- 77% of surveyed judges believe attorneys lack competence in e-discovery

SOCIAL MEDIA MAY BE PRESENT AT EVERY STAGE OF LITIGATION

Electronic Discovery Reference Model



INFORMATION GOVERNANCE





CORPORATE POLICIES

- We suggest incorporating company social media into document retention policies:
 - Determine length of time to keep records
 - Save metadata, date and time of post, content, and author
 - Archive posts in easily searchable central repository
- A proper retention policy can avoid discovery and authentication disputes during litigation
- Unlike other types of documents, retention may be out of your control as the documents post live by a third party
 - Train employees on expectations of policy

ADVISING CLIENTS ON INFORMATION GOVERNANCE

Draft policies with an eye toward possible litigation or enforcement actions (requires including all information that would be necessary in case)

Coordinate early and often with IT to ensure policy is being implemented on the ground

Know who is using social media on behalf of the company

Educate employees on the requirements of the retention policy to ensure the policy is being followed

IDENTIFYING AND PRESERVING SOCIAL MEDIA



DUTY TRIGGERED

- When a party knows or reasonably should know that information is relevant to claims or defenses in pending or reasonably anticipated litigation
- This can include any potentially relevant social media content
- FRCP 26(b)(1) and 37(e)
- *Nutrition Distrib. LLC v. PEP Research, LLC*, 2018 WL 3769162 (S.D. Cal. Aug. 9, 2018) (imposing sanctions on defendant for destroying relevant Facebook posts after a duty to preserve attached)



IDENTIFYING RELEVANT ESI

- Know your client
 - Corporate social media accounts and users
 - Relevant policies
- Know their business
 - Types of communications and information exchanged
 - Location of relevant employees
- Know the nature of the controversy
 - Types and formats of potentially relevant information
 - Posture and litigation outlook

IDENTIFYING RELEVANT ESI

- Involve e-discovery and IT resources (if available) at the start of the matter
- Plan custodian interviews that include specific questions about social media
 - Not: “Do you use social media in your business?”
 - Instead: “How do you communicate with your colleagues?”
 - “How do you share pictures and video with your colleagues?”
 - “What apps do you use on your phone or tablet to do business?”

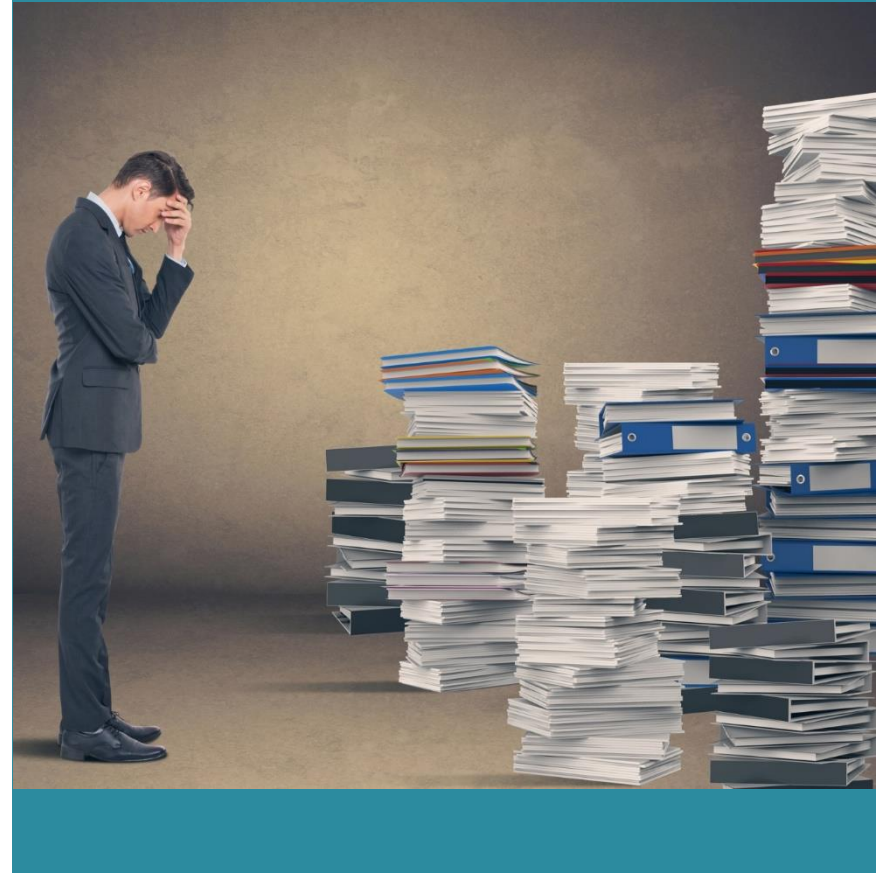


REASONABLE STEPS

- Duty to preserve any potentially relevant evidence in pending or future litigation
- Take all “reasonable steps” to preserve social media ESI (FRCP 37(e))
- What constitutes “reasonable steps” depends on the party’s knowledge at the time the preservation decisions were made
- Fact specific inquiry, but consider unique social media issues like:
 - Remote hosting
 - Difficulty in accessing data
 - Dynamic and collaborative nature of social media
 - Several types of data
 - Privacy issues

OTHER TIPS FOR PRESERVATION

- Be able to showcase to judge that a defined, replicable preservation process was used to help demonstrate you used “reasonable steps”
- Ensure litigation hold explicitly includes social media
- Employees will not consider social media “company records”
- Track and record all preservation activities
- Consider role of social media when selecting vendors
- Send document preservation letter to opposing counsel
- Identify key custodians early and conduct interviews quickly once duty to preserve is triggered
- Be aware of BYOD environments



CONTROL ISSUES

- Employers are considered to have control over content it creates and stores on either its own servers or third party servers
 - Recirculate litigation hold to remind employees posting for company to preserve data stored on third party platforms
- Employers generally don't have control over their employees' personal social media information
 - Requesting access to employee accounts from provider could violate SCA. See *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (awarding damages for violating SCA where employer used login credentials to access an employee's personal email account).
 - Could also violate state laws



Sanctions

NEXT EXIT

SPOILIATION AND SANCTIONS

- FRCP 37(e)
 - Deleting social media can result in severe sanctions
 - Unfavorable presumptions
 - Fines
 - Dismissal of action or default judgment
- But not if party has taken “reasonable steps”
- *Allied Concrete Co. v. Lester*, 285 Va. 295 (2013) (fining counsel \$542,000 and plaintiff \$180,000 for “cleaning up” client’s social media before responding to discovery request)

TIPS DURING PRESERVATION

On Offense

- Send document preservation letter to opposing party
- Possibility of sanctions under FRE 37(e) can be useful leverage

On Defense

- Have and follow a defined preservation plan
- Specifically include social media in lit hold
- Recirculate and update regularly
- Conduct custodian interviews early

COLLECTING SOCIAL MEDIA INFORMATION



TECHNICAL CHALLENGES WITH COLLECTION

- No such thing as “one size fits all” collection tools
- Collection tool flaws
 - Poor formatting
 - Poor compatibility with review platforms
 - Lost metadata
 - Authentication issues
- Talk to vendors about scope of case and your needs



COLLECTING INFORMATION IN CLIENT'S CONTROL

- What do you need to collect? → take reasonable steps to collect relevant information
- Client's posts and third parties' public posts can be collected
- Work to capture snapshot of relevant controlled material as quickly as possible. This includes:
 - Static image snapshots, self-collection from platforms, third party access through APIs, and WARC native files
 - Remember: social media files involve more than the content of posts (e.g. links and metadata)
- Balance cost-effectiveness with completeness of collection

SELF COLLECTION FROM PLATFORMS

- Various social media platforms have established means by which a user can download social media data.
- Data provided to user differs in form and appearance depending on the platform, e.g., Facebook, Twitter.
- May be preferable to have a vendor obtain the data using the appropriate tools and review the data in a manner including the available metadata.

ETHICAL CONCERNS



- Ethical rules may prohibit using phantom accounts or other deception to access and collect otherwise private social media content
 - Social media “stalking” or “false friending” involves deceit and misrepresentation, which can violate state ethic rules
- Risk of spoliation if collection alters relevant evidence

RESTRICTIONS ON COLLECTING THIRD PARTY'S PRIVATE INFORMATION

- The Stored Communications Act (SCA)
 - The SCA generally prohibits “a person or entity providing an electronic communication service to the public” from “knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service” 18 U.S.C. § 2702(a)(1)
 - SCA also prohibits disclosure by companies providing “remote computing services” to the public 18 U.S.C. § 2711(2)
 - Violating SCA can result in civil and criminal liability
- State laws may limit employer ability to demand username and password
- Many platforms have unique APIs that allow collection by a user of her own account

SCA CASE LAW

- The SCA has been interpreted to cover certain private social media content, such as private messages and non-public posts or comments:
 - See *Sines v. Kessler*, 2018 WL 3730434, at *2, *10 (N.D. Cal. Aug. 6, 2018) (quashing the portion of a subpoena seeking communications from a private, invite-only social networking and instant messaging platform because disclosure from the provider would violate the SCA); see also *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 667-68 (D.N.J. 2013) (holding that the SCA protected non-public wall posts on Facebook); *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012) (quashing a subpoena to Facebook for records from a deceased individual's Facebook account))
- Social media companies take the position that they are prohibited from disclosing private data, even by civil subpoena, without consent from the user. This position has often been upheld in court:
 - See *Chasten v. Franklin*, 2010 WL 4065606, at *2 (N.D. Cal. Oct. 14, 2010); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 975 (C.D. Cal. 2010); *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008)

STRATEGIES TO OBTAIN THIRD PARTY PRIVATE INFORMATION

- **BUT**: SCA only applies to platforms providing services to the public and only for the contents of private communications (i.e. communications not readily accessible to the public). This doesn't include the date, time, phone numbers or IP addresses
- Can also avoid violating SCA by subpoenaing the user or obtaining user's consent to access accounts or otherwise turn over information
 - Courts usually reject privacy claims if information is relevant and proportional
 - See, e.g., *Lewis v. Bellows Falls Congregation of Jehovah's Witnesses, Bellows Falls, Vermont, Inc.*, 2016 WL 589867, at *2 (D. Vt. Feb. 11, 2016)

TIPS DURING COLLECTION

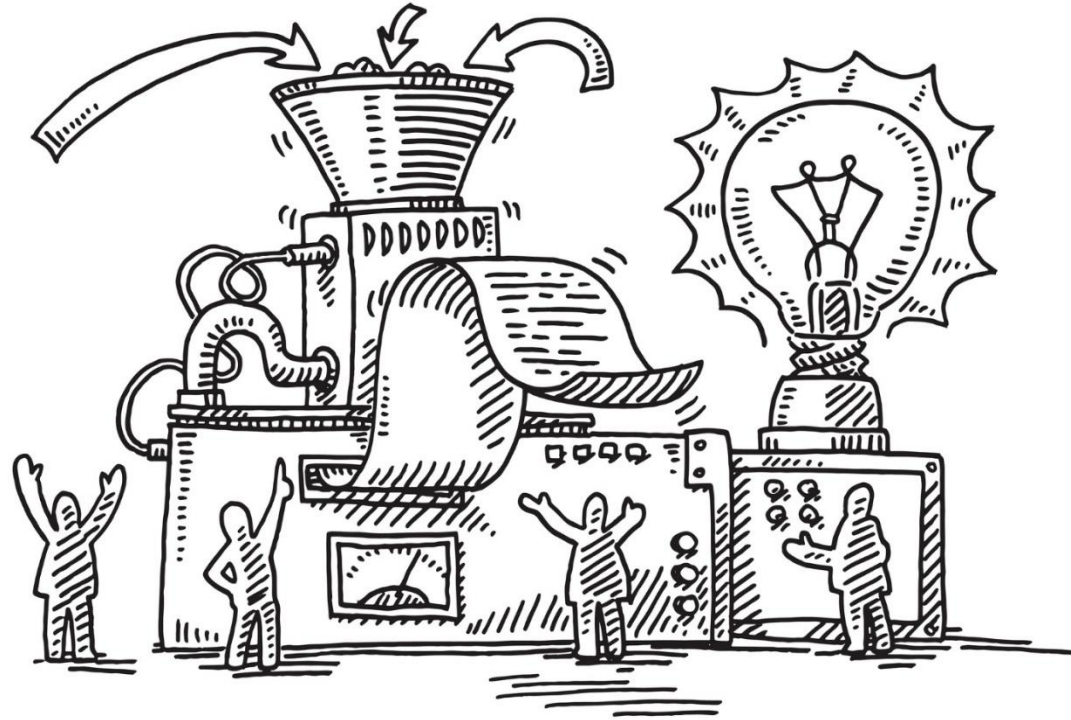
On Offense

- Seek out as much relevant public social media content as possible
- Check ethical rules on seeking access to non-public information
- Demand production from party, not third-party or employer

On Defense

- Advise clients on ways to maximize privacy settings
- Make backups to counter claims of alteration or spoliation
- Find vendor that can satisfy your needs

REVIEW & PRODUCTION



REVIEWING DATA

- Driven by how data was preserved and collected
- Once data is collected, converting it into useable and most useful format for review requires discussion of the needs of the case and what data is meant to show
 - Will parties need to review data interactively? → use API or WARC native files
 - Is a static image/screenshot sufficient? → e.g. incriminating Twitter post (ok) v. video post (no)
 - Are you interested in the metadata?
 - Be aware of change in content over time

VOLUME OF DATA

- Small data volumes easier to get API interactive files
- For large data volumes experienced vendors and specialized tools will be helpful
 - Filter content early with review tools (best for text)
 - Data clustering and near duplicate identification technologies
 - More advanced review platforms combine different social media files and data in one place for easy review



PRODUCING DATA

- Format of data you'll produce to opposing party depends on what's needed
 - Copy of native file or API
 - Access to login information
 - Static images/screenshots
 - "Friend" or "follow" the party (beware of ethical concerns) or provide log-in information
- Cooperate with opposing party and avoid gamesmanship
- Consider using a vendor to narrow production to just relevant information and streamline process

TIPS DURING PRODUCTION

On Offense

- Choose vendor carefully based on needs of case (e.g. content type and volume of data)
- Request AMI and native files
- Cooperate

On Defense

- Consider file formats for production (prefer static images)
- Cooperate

RULE 26 – RELEVANCE AND PROPORTIONALITY CONSIDERATIONS



RELEVANCE & PROPORTIONALITY

- FRCP 26(b)(1): evidence is discoverable if it is relevant and proportional to the needs of the case
- Social media may be relevant and proportional to many aspects of a case
- Courts have found that private messages and posts can be relevant and proportional
 - See *Forman v. Henkin*, (N.Y. Ct. App. Feb. 13, 2018) (finding pre- and post-accident photos privately posted on social media were relevant and not unduly burdensome); *Nucci v. Target Corp.*, 162 So. 3d 146, 148, 152 (Fla. Dist. Ct. App. 2015) (holding that photographs from plaintiff's Facebook page could be relevant to his claim for personal injury damages)



BUT DON'T ABUSE

- “Fishing expeditions” and unfettered access still discouraged
- *United States ex rel. Reaster v. Dopps Chiropractic Clinic, LLC*, 2017 WL 957436 (D. Kan. Mar. 13, 2017)
- Judges disapprove of gamesmanship



WHERE'S THE LINE?

On Defense

- Focus on proportionality and relevance → Fishing expedition? Unfettered access?
- Possible *in camera* review by judge to limit scope
- Have social media policy for company
- Use privacy and proportionality arguments

On Offense

As the requesting party, find a balance →
be reasonable
Show it's relevant
Proportional to needs of case
Be aware of locational data

LIMITS

Same discovery principles apply

Identify issues at early Rule 26(f) conference

Judges stress cooperation

Courts balance relevance against fishing expeditions

PRIVATE INFORMATION IS NOT A BAR TO DISCOVERY

- Private content ≠ not discoverable
 - If it's relevant and proportional to the needs of the case a judge could rule it is discoverable
 - *A.D. v. C.A.*, 50 Misc. 3d 180 (N.Y. Aug. 13, 2015) (stating that “[a] person’s use of privacy settings on social media, such as Facebook, restricting the general public’s access to private postings does not, in and of itself, shield the information from disclosure if portions of the material are material and relevant to the issues of the action”)
- But a judge can determine that a party’s privacy interests outweigh the need for the information
 - *Henson v. Turn*, 2018 WL 5281629 (N.D. Cal. 2018) (finding plaintiffs’ privacy interests in their smartphones and computers outweighed defendant’s interest in searching those devices for relevant information).

LIMITS

Other limiting factors to consider:

Rule 26(b)(2)(c)
factors limiting
discovery

Protective orders
under Rule 26(c)(1) to
avoid embarrassment,
oppression, or undue
burden

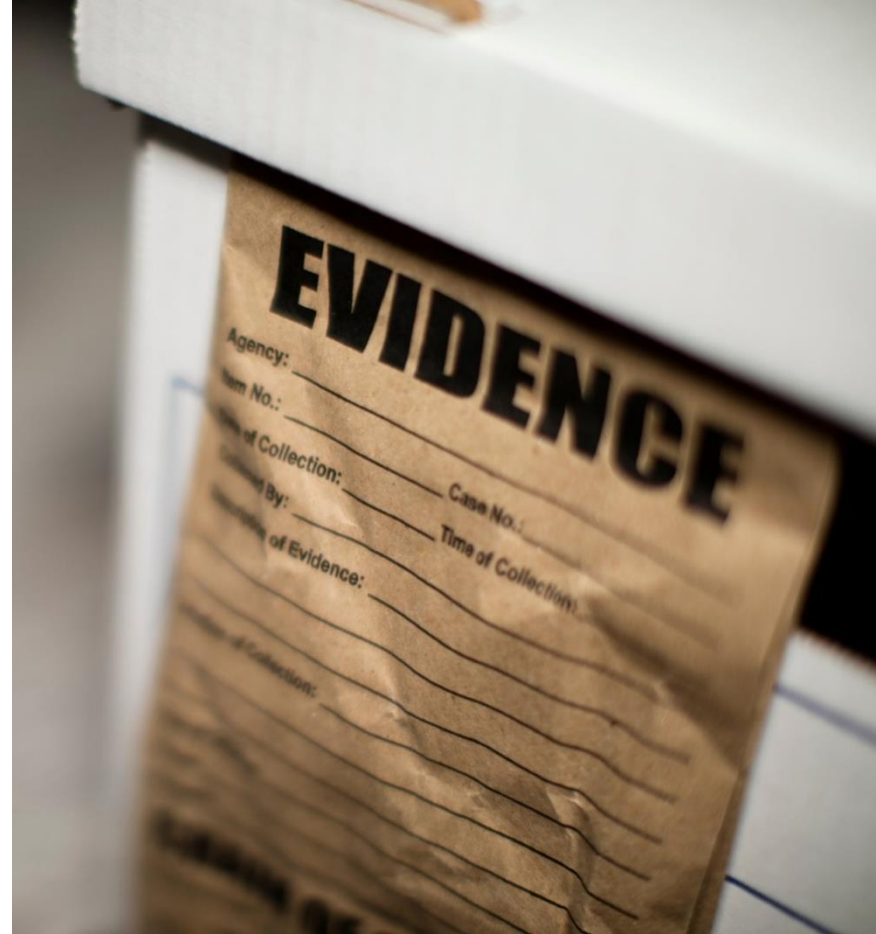
International privacy
laws

USING SOCIAL MEDIA AS EVIDENCE



AUTHENTICATION

- Authenticating social media evidence should be considered during collection, processing, and production
 - Screenshots may be inadmissible without authentication
- FRE 901 and basic evidentiary rules apply
- Preservation of metadata is key for admissibility
- Self-authentication and FRE 902
 - New FRE 902(13) and (14)



RECENT CASE LAW

- Most courts have adopted a test similar to authentication for other forms of evidence
- Authentication based on any type of evidence to demonstrate to the trial judge that “a jury could reasonably find that the proffered evidence is authentic”
 - See, e.g., *United States v. Vayner*, 769 F.3d 125, 129–30 (2d Cir. 2014); *Sublet v. State*, 113 A.3d 695, 698, 718, 722 (Md. 2015)
- But mere testimony of the person who downloaded/printed the content, without more, will likely not authenticate material

QUESTIONS?





Kristen A. Lejnieks
Partner
kalejnieks@jonesday.com
+1.202.879.3703



One Firm WorldwideSM



Theresa M. Coughlin
Associate
tcoughlin@jonesday.com
+1.202.879.3617



DISCLAIMER

- Any presentation by a Jones Day lawyer or employee should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its content is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of Jones Day.