Building Your Case with Electronic Evidence: Facebook, Text, Email Evidence and More

For information on how to become a faculty member for one of our seminars, contact the Planning Department at the address below, by calling **(800) 777-8707,** or emailing us at speakerinfo@nbi-sems.com.

NBI, Inc.
PO Box 3067
Eau Claire, WI 54702

77864

IN-HOUSE TRAINING

Can training your staff be easy **and** individualized?

It can be with NBI.

Your company is unique, and so are your training needs. Let NBI tailor the content of a training program to address the topics and challenges that are relevant to you.

With customized in-house training we will work with you to create a program that helps you meet your particular training objectives. For maximum convenience we will bring the training session right where you need it…to your office. Whether you need to train 5 or 500 employees, we'll help you get everyone up to speed on the topics that impact your organization most!

Spend your valuable time and money on the information and skills you really need! Call us today and we will begin putting our training solutions to work for you.

800.930.6182

Jim Lau | Laurie Johnston

Legal Product Specialists
jim.lau@nbi-sems.com
laurie.johnston@nbi-sems.com

NBI | NATIONAL BUSINESS INSTITUTE

www.nbi-sems.com

Building Your Case with Electronic Evidence: Facebook, Text, Email Evidence and More

Authors

Camille E. Blanton
The Law Office of Camille Blanton, PLLC
Charlotte, NC

Leila A. Hicks
Law Offices of James Scott Farrin
Durham, NC

Brian W. King
King Law Offices PLLC
Rutherfordton, NC

Corey V. Parton
Parton & Associates, PLLC
Charlotte, NC

Presenters

CAMILLE E. BLANTON is an attorney in private practice in Charlotte with The Law Office of Camille Blanton, PLLC. She focuses her practice on the advocacy of those who have been harmed by the negligence of others. Ms. Blanton is admitted to practice law in all North Carolina and Florida state courts, as well as before the U.S. District Court for the Western District of North Carolina. She has written and instructed continuing education classes to insurance claims adjusters in North Carolina, Florida, and Texas. Ms. Blanton attended the University of North Carolina at Chapel Hill, where she earned a degree in psychology. Ms. Blanton then moved to Florida, where she attended the University of Miami School of Law.

LAURA H. BUDD is the managing partner of The Budd Law Group, PLLC, where she practices in the areas of civil litigation, family law, and estate planning and administration. She is admitted to practice in North Carolina for the 4th Circuit in the Western District of North Carolina. Ms. Budd is a member of the American Bar Association, North Carolina Bar Association, North Carolina State Bar, American Association for Justice, Mecklenburg County and Union County bar associations. She earned her B.A. degree, cum laude, from The Ohio State University and her J.D. degree from Wake Forest University School of Law. Ms. Budd has taught multiple CLEs in family law and business law over the years on a wide range of topics. She also is a certified superior court mediator.

BRIAN W. KING is a senior partner with King Law Offices, LLC, and has more than 20 years of litigation experience. Mr. King has been a North Carolina family law specialist for nine years. He has been a frequent speaker on family law issues, including a regular speaker at the North Carolina Child Support Conference in the past. His firm has 12 offices located across Western North and South Carolina. Mr. King has represented more than 1,000 domestic law cases personally. He has experience in a broad range of cases, including contracts, claims, litigation, mediation, and arbitration. Mr. King is admitted to practice in North Carolina and South Carolina. He is a member of the North Carolina State Bar, South Carolina Bar, and several other North and South Carolina bar associations, and served as District Bar president. Mr. King earned his B.A. degree from the University of North Carolina at Charlotte and his J.D. degree from Campbell University.

COREY V. PARTON is the founder and managing partner at Parton & Associates, PLLC. He has practiced law in Charlotte, North Carolina since 2013, winning settlements for his clients in the areas of commercial litigation and finding the best possible outcomes for his clients facing charges in criminal defense. Mr. Parton serves as the vice-chair on the Board of Directors for the Mecklenburg County Bar's Lawyer

Presenters (Cont.)

Referral Service and is a member of the Mecklenburg County Bar Sports Committee. He is a member of the Bar of the Supreme Court of the United States, Mecklenburg County Bar's Criminal Defense & Small and Solo Practice sections, has served as a judge for the Carolinas Cup Trial Team Competition, and has been featured on Charlotte's *WBTV-3* and *Time Warner Cable News* as a legal consultant. Mr. Parton has been recognized by *Super Lawyers* as a Rising Star, with an Outstanding Teacher Award for his volunteer work teaching English as a Second Language to Adults and has been published by the American Bar Association and Charlotte School of Law's Civil Rights Clinic. He received his B.A. degree from Virginia Tech and earned his J.D. degree from Charlotte School of Law.

Table Of Contents

What to Look For

Submitted by Camille E. Blanton

I. What to Look for

A. Different Types of Electronic Data

Electronically stored information (ESI) is any information that is stored in an electronic format, versus a traditional format (such as paper). The identification and use of such information/data is vital not only to the investigation and building of a case, but to the pre-screening of clients and determination of the strengths and weaknesses of their potential claims. This information may be stored in something as simple as a personal or office hard drive, to something more complicated that involves the retrieval of metadata previously erased by a corporate entity.

B. Different Electronic Formats – in Detail

1. Hard Drive – A hard drive is a digital data storage device that stores and retrieves data using rotating disk coated with magnetic material. It is typically defined by the characteristics of capacity (measured in terabytes or gigabytes and performance (access time and latency time). If seeking information from a traditional computer, this is generally the initial search item at issue.
2. Vaulting – This is a form of off-site data protection (back-up), which is less common now that e-vaulting (cloud-based storage) is readily available and generally more financially feasible. For examples, Florida hurricanes (discussed).
3. Laptop/Notebook/Tablet - The portability and near weightlessness of personal computers (including notebooks and tablets) have vastly increased the number of purposes each may serve. In examining the same, you must consider privacy settings and stored data. This may include not only those applicable to personal and professional data, but also that of shared users, such as family and/or household members.
4. Email/Instant Messaging – When discussing email, which must also be considered with respect to personal, professional and/or shared use, personal messaging sites/applications must also be examined. For example, WhatsApp, Skype and Viber (discussed).
5. Cloud - Personal/Home-Share/Work

6. Social and Professional Social Media – For example, Facebook, Instagram and LinkedIn (discussed).
7. Listserv Groups (Personal/Professional) – Privacy concerns/expectations.
8. Blog (Weblog) – For example, Wordpress.
9. Photoblog – For example, Pinterest and Instagram.
10. Vlog (Video Weblog) – For example, YouTube.
11. Message Boards (Private/Public) – Privacy concerns/expectations.
12. Podcasts – Podcasts operate somewhat as the radio of today, but specifically refer to digital broadcasting series.
13. Cell Phone/Personal Digital Assistant (PDA) – These devices are being addressed last, because in discussing, all of the above noted privacy and shared use considerations applies, as well as the specific types of data examined individually. In fact, there is very little ESI that cannot be collected and/or accessed via a cell phone or PDA.

C. Identifying Relevant Systems and Data

The above discussed are but a sampling of the items your checklist should include when interviewing a potential client, conducting written or deposition discovery and/or examining a witness at trial. Once identified, you will need to preserve and/or protect any potential electronic evidence at issue. Doing so with respect to opposing parties or witnesses can be accomplished through the manner/methods discussed in section I of this seminar. If discussing this matter with your client, the safest option is to have her review all potential electronic evidence in your presence. You should do so with attention to detail in examining any creative/non-traditional data, as well as family/work ESI in addition to personal devices. If your client permits, an examination and copy of the information stored on any relevant SIM (subscriber identity module) card available may provide you with easy access to some or all of this information.

You may also consider hiring a forensic examiner to collect the data sought, particularly if in the possession of an opposing party, third party or witness. Such an expert may ensure an unbiased collection and examination of the data desired of your client. The North Carolina Office of Indigent

Defense Service has a database of experts available for viewing at http://www.ncids.com/forensic/experts/experts.shtml.

Further, the material discussed today is a very broad overview of what you, as an attorney, need to know about digital forensics and the ever-growing impact it may have on the way in which you practice law. Thus, a detailed and more in depth study is highly recommended. *See* Daniel Larry, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom* (1st ed. 2012); Linda Volonino and Reynaldo Anzaldua, *Computer Forensics for Dummies* (1st ed. 2008); and Shira Scheindlin and Daniel Capra, *Electronic Discovery and Digital Evidence in a Nutshell* (1st ed. 2009). *See also* Amelia Phillips, Ronald Godfrey, Christopher Steuart and Christine Brown, *E-Discovery: An Introduction to Digital Evidence* (1st ed. 2014), which includes an interactive DVD that allows you to work with e-discovery and forensic tools, as well as several data processing and review platforms.

D. Who are You Going to get the Data From?

1. Client - Depending on your relationship with a particular client, as well as her willingness and/or ability to assist you with the collection of ESI, data collection software or a device application may be useful. A basic search engine query will provide you with a number of choices for collection of data from the devices discussed thus far, but you should always review applicable privacy and privilege laws prior to use.

2. Working with and Subpoenaing Social Media Companies - Your approach to obtaining data from social media companies will differ, depending on your needs and the policy and procedures of each entity. Of utmost importance in the issuance of a subpoena, is using language that specifically and sufficiently describes the data sought, while narrowing tailoring the same to prevent an argument of undue burden (physical or financial) in opposition. In 2010, the North Carolina Court of Appeals discussed this matter in detail, and issued what may be considered a reprimanding opinion. *See* Kelley v. Agnoli 205 NC. App. 84 (2010).

The information needed to create and serve subpoenas for most social media websites is typically found via a link on the home page, commonly referenced as legal or law enforcement information. Below you will find links for a number of the social media sites discussed today:

i. Twitter: https://support.twitter.com/articles/41949#8:
ii. Facebook: https://www.facebook.com/help/473784375984502;
iii. Instagram: https://help.instagram.com/494561080557017/;
iv. LinkedIn: https://www.linkedin.com/legal/privacy-policy;
v. Google: http://www.google.com/transparencyreport/userdatarequests/legalprocess/;
vi. Pinterest:https://help.pinterest.com/en/articles/law-enforcement-guidelines;
vii. Tumblr: https://www.tumblr.com/docs/en/law_enforcement;
viii. Snapchat: https://www.snapchat.com/static_files/lawenforcement.pdf; and
ix. WhatsApp: http://www.whatsapp.com/legal/.

3. Facebook's Archive Feature - Facebook provides you with the unique ability to download archived information using the "Download Tool" (https://www.facebook.com/ help/131112897028467/). At this time, there does not appear to be a feature that allows for the selection of data sought, thus you must download your file in its entirety (zip drive formatted). The amount of information may be overwhelming, depending on the amount of time the account has been open and extent of use.

4. Using Friending/Following to Obtain Info - The practice of "Friending" or "Following" to obtain information must be addressed in conjunction with the ethical implications of doing so. Thus, North Carolina Rules of Professional Conduct, Rule 8.4 and North Carolina State Bar Formal Ethics Opinion 7 (2014) should be taken into consideration unless the act at issue is done so with the express permission of your client (or other). If

not, you must determine whether or not the information is readily available for public viewing and/or may be obtained other than using fraudulent means.

5. Closed Accounts - Once an account has been closed, your only options are to either forward an executed consent request or a subpoena to the service/entity custodian. Depending on the service at issue and the amount of time that has passed since the account was closed, the data may or may not be available. The American Civil Liberties Union maintains a cell phone data retention chart, which lists the time periods of retention for categories of data with respect to the major cellular service providers.

6. Obtaining Deleted Data - With respect to the pursuit of deleted data, all methods discussed thus far may be employed. However, a digital forensic examiner should be utilized unless you have complete knowledge of the extent and location(s) of the deleted data being sought.

7. Emails (Work-Related and Personal) - With respect to your own client, the issues of identification, preservation, spoliation and authentication discussed above apply in this arena, as have the methods of identifying and obtaining the same from an opposing or third party. Throughout review and/or production, one must continue to consider the ethical issues and applicable privacy laws involved in both work and personal emails. In addition, the importance of maintaining completely separate work and personal emails accounts, as well as implementing work place policies and procedures within your own firms and/or the businesses of your clients, should be emphasized.

8. Video Surveillance (Private and Public) - The consideration of public versus private is of issue is in the process of viewing and/or obtaining video surveillance footage. Similar to the prior forms of data discussed, your method will likely depend on the source or custodian of the footage, and whether that person is your client or an opposing/non-party. Further, with respect to private surveillance (non-protected), you should first employ the simple method of asking for it. However, if/when permission is granted, you must take all necessary measures to ensure that the physical method(s) of retrieval and storage are sufficient to withstand any

anticipated evidentiary challenges. This is often the primary reason for hiring a private investigator to obtain surveillance. Such a person is well versed in the manner in which it should be done to ensure admissibility, and will testify as to the same.

9. Computerized Versions of Contracts and Other Documents

10. Electronic Signatures - With respect to the validity of electronic signatures in execution of contracts, the most recent policies discussed by the North Carolina Department of the Secretary of State on this matter, may be viewed at https://www.secretary.state.nc.us/ecomm/. In summary, electronic signatures should be:

a. unique to the person signing;
b. capable of certification;
c. controlled solely by the person signing;
d. invalidated if data is altered; and
e. conforms with rules adopted by the Secretary of State.

See Electronic Commerce Act, N.C.G.S. § 66-58.1.

11. Text Messages and Voicemail

a. Opposing/Non-Parties - This matter was covered in some detail during Section II. Please note the cellular service provider chart referenced therein, as an executed request for records or court issued subpoena to the relevant service provider will often be your only option with respect to obtaining opposing or non-party text messages and voicemail.
b. Client Owner/Operator - Some cell phones and PDAs inherently have the ability to forward digital voicemails via text and/or email, but the action is typically limited to communication with a compatible device within the same network. If the message and/or voicemail at issue is owned by your client, you may require a program or application for access, preservation and storage.
c. Reference Materials – Our discussion of this subject matter is subject to time constraints, but there are a number of materials

available that offer a detailed explanation and analysis of the art of cellular investigation. *See* Aaron Edens, *Cell Phone Investigations: Search Warrants, Cell Sites and Evidence Recovery* (1st ed. 2014).

12. Chats and Instant Messages - In addition to the above discussed methods related to text messages and voicemails with respect to your own client, the use of a screen shot or page save may be utilized in the access, preservation and storage of chat and/or instant message (IM) data (interactive use/example).

E. Privileged ESI That is Discoverable (Exceptions) – I mentioned that we would continue our discussion of computerized versions of contracts and other documents in the following section, wherein we have to examine metadata/privilege concerns with respect to discoverable electronic evidence. It is becoming more and more common to negotiate, edit and agree upon the terms and content of contracts via email. If you are the creator of the contract or document at issue, you must take all necessary measure to ensure that no metadata (unless intended) is transmitted during email exchange. For example, you may want or need to retain information noting when and what information was edited, and by whom. However, any edits made by your client and/or administrative notes regarding client input or other privileged information must be protected. If this is a practice allowed and utilized within your firm or practice, all employees should be trained with respect to the same. In addition, you may wish to address the same within a policies and procedures manual provided to employees.

Metadata Explained

Submitted by Camille E. Blanton

II. Metadata Explained

Simply put, metadata is data that describes or summarizes basic information about other data. Metadata may provide information such as the way specific data was created, the date and time of creation, its purpose and/or the author of the data. The use and application of metadata in electronic discovery is both complicated and ever-evolving.

a. Defining Different Types and Formats

i. Descriptive – Examples: Key words, author, abstract and location (geotags).
ii. Structural – Example: Data about the way the data is organized.
iii. Administrative – Example: Facilitator notes.

b. Metadata Landmines to Avoid

Pitfalls and cautionary tales are many, but common error in metadata is one that every person in this room has likely made at least once. If you have ever emailed a Word, Excel, PowerPoint or WordPerfect file/document to opposing counsel, chances are that you have also shared unintended data. We will examine a sample document received via email using Microsoft Word:

i. Open the email attachment;
ii. save the document;
iii. right click on the file;
iv. click on Properties; and
v. view each tab.

c. "Scrubbing" Metadata to Remove it from Documents

If you found the above example disturbing, you should begin implementing standard precautionary practices to ensure the safety and privacy of your files. The way in which files are stored will determine the method necessary to remove the metadata that is automatically stored, which has the potential for unintended transmission. With respect to the Word document just viewed, the easiest way to prevent transmission of metadata is to simply save it as a PDF, or scan a paper copy of the document and send it via email/fax. However, if you need the intended recipient to have the ability edit the document, certain program features may be changed to achieve this. For example, if you are using Word, PowerPoint or Excel, you can uncheck the "Fast saves" option. You may also obtain a security program

through your software provider, or purchase a data scrubber/removal program. While time will not permit us to delve further into this topic, you should be mindful of this issue when seeking discovery from an opposing party and/or reviewing documents provided, which may contain metadata.

The safest way to address the production of your own metadata pursuant to the request of opposing counsel is via a forensic examiner. In lieu of doing so, or in preparation of the same, you should follow some basic steps:

a. Retain – You may do so by obtaining consent and access;
b. Search and Secure – Review the information as discussed above and copy the same;
c. Document – Note the way in which all data was accessed, so as to preserve the chain of custody in anticipation of challenges;
d. Examine/Interpret – Determine the specific nature and content of all information found;
e. Analyze/Describe – Upon analysis of the data at issue, describe it broadly and narrowly; and
f. Respond/Protect – Consider each item individually, noting if it is responsive, as well as any applicable privilege.

What to Look for, Where to Find it and What to do With it: Email, Social Media, Texts and Video

Submitted by Leila Hicks

WHAT TO LOOK FOR, WHERE TO FIND IT AND WHAT TO DO WITH IT:

EMAIL, SOCIAL MEDIA, TEXTS AND VIDEO

SUBMITTED BY LEILA A. HICKS

FEB. 2016

A. TYPES OF DATA, PRODUCTION SPECIFICATIONS AND FORMATS – IN DETAIL

a. What is "Data"?

i. "Computer data is information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's CPU and is stored in files and folders on the computer's hard disk." (TechTerms)

ii. Electronically Stored Information ("ESI")

b. Types of Data

Messages - Images - Audio Clips - Video Clips – Locations - Search History – Personal Information

c. Production Specifications and Formats

i. Selecting the Form of Production

1. Pursuant to NCRCP Rules 34 and 45, Discuss With Opposing Counsel the Form or Forms of Production in Document Requests or a Subpoena
2. There Are Different Forms of Production That Are Appropriate for Various Forms of ESI But Need Not Produce the Same ESI In Numerous Forms
3. If the Parties Cannot Agree With the Form of Production, Production Should Be the Form in Which it is Ordinarily Maintained (Typically the Native Format) or a Reasonably Usable Form
    a. Be Aware That The Ability to Produce in a Reasonably Usable Form Does Not Allow the Producing Party to Convert the ESI Form to Make Utilization of the ESI Difficult for the Requesting Party

ii. Formats

1. Native Format
    a. Responsive ESI in the Form That it is Ordinarily Maintained on the Producing Party's Systems and it Usually Includes the Metadata Associated With the ESI.
2. Near-Native Format
    a. Some Files, Including Email and Large Databases, Cannot Be Reviewed For Production or Produced Without Some Form of Conversion.
    b. In Near-Native Format, Files Are Extracted or Converted Into Another Searchable Format.
3. Image (Near-Paper) Format
    a. The ESI is Converted So That a "Picture" is Taken of the ESI as it Might Exist if it Were in Paper Format or Viewed On-Screen.
4. Paper Format
    a. Paper or "Hard Copy" Documents Are Physical Documents Copied From Other Physical Documents or Printed From ESI

B. OBTAINING EVIDENCE: SMARTPHONES, PCS AND TABLETS, THIRD PARTIES, FLASH DRIVES AND EXTERNAL HARD DRIVES, CLOUD STORAGE

a. PCs (Personal Computers)

i. What Is It?

1. A General Purpose Computer That is Intended to Be Used By A Consumer For Various Functions

ii. How to Obtain Data From PCs

1. For Intact Hard Drives, Search the Hard Drive and Extract Files in a Compressed ZIP File
2. For Damaged or Corrupted Hard Drives, Obtain Assistance From the Manufacturer or Utilize a Professional Data Recovery Service

b. External Hard Drives
    i. What Is It?
        1. A Portable Data Storage Device That Can Be Attached to a Computer Through a USB, FireWire Connection or Wireless Connection. External Hard Drives Typically Have High Storage Capacities and Are Often Used to Back Up Computers.
    ii. How to Obtain Data From External Hard Drives
        1. For Intact External Hard Drives, Search the External Hard Drive and Extract Files in a Compressed ZIP File
        2. For Damaged or Corrupted External Hard Drives, Obtain Assistance From the Manufacturer or Utilize a Professional Data Recovery Service
c. Tablets
    i. What Is It?
        1. A Wireless, Portable Personal Computer With a Touchscreen Interface.
    ii. How to Obtain Data From Tablets
        1. For Intact Tablets, Back Up Information to an External Hard Drive or Upload to a Cloud Storage Service
        2. For Damaged or Corrupted Tablets, Obtain Assistance From the Manufacturer or Utilize a Professional Data Recovery Service
d. Smartphones
    i. What Is It?
        1. A Cellular Phone That Performs Many of the Functions of a Computer
    ii. How to Obtain Data From Smartphones?
        1. For Intact Smartphones, Back Up Information to a Cloud Storage Service
        2. For Damaged or Corrupted Smartphones, Obtain Assistance From the Manufacturer or Utilize a Professional Data Recovery Service

e. Flash Drives
    i. What Is It?
        1. A Portable Data Storage Device That Can Be Attached to a Computer Through a USB Connection and Can Be Easily Electronically Erased and Reprogrammed.
    ii. How to Obtain Data From Flash Drives?
        1. For Intact Flash Drives, Upload Information to a PC or External Hard Drive or Back Up Information to a Cloud Storage Service
        2. For Damaged or Corrupted Flash Drives, Obtain Assistance From the Manufacturer or Utilize a Professional Data Recovery Service
f. Cloud Storage
    i. What Is It?
        1. A Means of Data Storage in Which Digital Data is Stored Remotely And Made Available to Users Over a Network
    ii. How to Obtain Data From Cloud Storage?
        1. For Intact Cloud Storage Accounts, Access the Cloud Storage Account and Download Information to PC, External Hard Drive, or Flash Drive
        2. For Corrupted or Deleted Cloud Storage Accounts, Obtain Assistance From the Cloud Storage Provider or Utilize a Professional Data Recovery Service
g. Parties and Third Parties
    i. From Whom Should You Obtain Information?
        1. Parties and Third Parties With Non-Privileged Information That is Relevant to the Litigation
    ii. How to Obtain Data From Third Parties?
        1. Parties
            a. Discovery
                i. NCRCP Rule 26
        2. Third Parties
            a. Subpoena
                i. NCRCP Rule 45

C. USING APPS ON YOUR CLIENT'S SMARTPHONE TO COLLECT EVIDENCE

a. Why Collect Evidence on Your Client's Smartphone?
    i. Modern Mobile Phones Often Have Large Storage Capacities and Unless Thoroughly Erased From the Device, the Data Remains on the Device
    ii. Data in Smartphones Can Be Referred to as Electronically Stored Information ("ESI"). ESI in Smartphone Apps Have the Same Ability to be Introduced at Trial and Admitted Into Evidence and Therefore is Discoverable
    iii. Attorneys May Be Required to Preserve Evidence and Prevent Spoliation
        1. See Below

b. Apps That Collect Electronically Stored Information ("ESI")
    i. Standard Smartphone Utility Apps

        Text Message - Address Book - Call History – Voicemail – Notes - Voice Memo – Email

    ii. Cloud Storage Apps

        Dropbox - One Drive – Box – iCloud - Google: Photo, Drive, Vault, Photo, Docs, Sheets

    iii. Social Media Apps

        Facebook – Facebook Messenger – Snapchat – Twitter – Instagram

    iv. GPS Location Apps

        iPhone Maps - Google Maps – Uber – Lyft

c. Practice Tips
    i. Be Aware of What Your Client's Smartphone Apps Do
        1. Having Knowledge of the Function and the Features of the App Will Allow You to Properly Advise Your Client and Anticipate What Information Maybe Discoverable
    ii. Prevent Spoliation (Back Up Information or Protect the Device From Loss or Destruction)
        1. If Relevant ESI is Destroyed in Anticipation of Litigation, Clients May Be Subject to Sanctions and Default Judgments and Attorneys May Be Subject to Sanctions

iii. Advise Your Client to Be Aware of What They Post On Social Media But Warn of Intentional Deletion of ESI

iv. Consider an eDiscovery App Like Google Vault

d. Case Law

i. *Aggreko, LLC v. Koronis*, Civil Action No. 13-13034-TSH (D. Mass. Dec. 19, 2013)

ii. *Calderon v. Corporation Puertorriue A De Salud*, 2014 WL 171599 (D. Puerto Rico Jan. 16, 2014)

iii. *PTSI, Inc. v. Haley et al.*, 2013 PA Super 130, No. 684 WDA 2012

iv. *Garcia v. City of Laredo, Tex.*, 2012 WL 6176479 (5th Cir. Dec. 12, 2012)

D. PREDICTIVE CODING DO'S AND DON'TS

a. What Is Predictive Coding?

i. The Use of a Keyword Search, Filtering and Sampling to Locate Desired Information and Therefore Reduce the Number of Documents That Need to Be Reviewed Manually By Sorting Out Irrelevant and Non-Responsive Data

b. Predictive Coding Terminology

i. Precision

1. The Measurement Within the Selected Set of the Ratio of Relevant Documents to the Total Number of Selected Documents. High Precision Indicates Effectiveness of the Search Whereas Lower Precision Indicates a Larger Number of False Positives.

ii. Recall

1. The Measurement of the Number of Relevant Documents Within the Selected Set Versus the Total Number of Relevant Documents Within the Entire Body of Documents Available.

iii. Linear Review

1. The Traditional Methodology For Document Review. Through Linear Review, Documents Are Reviewed in the Exact Order in Which They Were Stored and Delivered to the Review Team.

iv. Non-Linear Review

1. The Review Methodology That Attempts to Leverage Any Information About a Document or Contained Within a Document to Attempt to Improve the Review Process.

v. Supervised Learning

1. An Algorithm That Learns From Human Decisions and The Has the Ability to Apply Those Decisions to New Data. A Training Set is Utilized to Allow the Algorithm to Apply Human Decisions to Automated Decisions.

vi. Unsupervised Learning

1. An Algorithm That Can Analyze Data Without Needing a Training Set. The Algorithm Can Discern Patters Within the Data.

vii. Prioritized Review

1. A Selection Methodology That Moves Presumed Relevant Documents to the Front of the Analysis Line. Subsequently, Human Review is Conducted to Review Rankings of Presumed Relevant Documents and Re-Rank Documents Based on Relevance.

viii. Automated Review

1. In Contrast With Prioritized Review, Document Selection is Made Without Subsequent Human Review of Relevance Rankings.

ix. Search Terms

1. Textual Strings That Are Used To Search Within a Body of Information. Search Terms Can Be Done in Documents That Have Been Indexed or That Have Not Been Indexed.

x. Sampling

1. A Selection Methodology That Reviews a Portion of the Information That Allows the Reviewer to Make a Decision Against the Larger Population.

xi. Search Engine Optimization

1. The process by which web pages and embedded terms can be adjusted or modified to maximize performance in specific searches on search engine sites like Google, Yahoo, and Bing.

c. Practice Tips

i. Do

1. Prioritize Pre-Production Review to Identify the Universe of Potentially Relevant Documents Then Use Predictive Coding to Organize and Prioritize the Review of Those Documents
2. Sort Documents By Potential Privilege By Ranking the Likelihood That Particular Documents Are Privileged
3. Quality Control a Planned Production of Documents By Utilizing Multiple Search Methods on the Same Set of Documents to Assess Whether Search Decisions on Relevance or Privilege Need to be Modified

ii. Don't

1. Assume All Predictive Coding Programs Are Created Equal
2. Underestimate the Need For Experienced Attorney Oversight

E. METADATA EXPLAINED

a. Defining Different Types and Formats

i. What is Metadata and Why Does It Matter?

1. Often Referred to as "Data About Data", Metadata is a Set of Data That Describes and Gives Information About Other Data (ex: File Creation Date Stamp on a Document)

2. Because This Information is Hidden Within the Digital Copy of a Document, File, Photo or Other Piece of Information That is Often Transmitted Between Parties, Attorneys and Clients Need to Be Aware of the Metadata That May Be Transmitted Along With the Digital Data Type

b. Metadata Landmines to Avoid

i. North Carolina State Bar Ethics Committee 2009 Formal Ethics Opinion 1

1. "Reasonable Precautions"

a. The State Bar's Ethics Committee Stated That "A Lawyer Who Sends an Electronic Communication Must Take Reasonable Precautions to Prevent the Disclosure of Confidential Information, Including Information in Metadata, to Unintended Recipients"

2. What Is Reasonable?

a. It Depends On:

i. The Sensitivity of the Confidential Information That May Be Disclosed

ii. The Potential Adverse Consequences From Disclosure

iii. Any Special Instruction or Expectations of a Client

iv. The Steps That The Lawyer Takes to Prevent the Disclosure of Metadata

ii. May Attorneys Searching For (aka "Mine") Metadata? No.
    1. Interference With Client-Lawyer Confidentiality
        a. "A lawyer May Not Search For Confidential Information Embedded in Metadata of an Electronic Communication From Another Party or Lawyer For Another Party. By Actively Searching For Such Information, A Lawyer Interferes With the Client-Lawyer Relationship of Another Lawyer and Undermines the Confidentiality That is the Bedrock of the Relationship."

iii. Receiving Attorney's Duty to Metadata Sender
    1. Duty to Notify Party or Party's Counsel
        a. "If a Lawyer Unintentionally Views Confidential Information Within Metadata, the Lawyer Must Notify the Sender and May Not Subsequently Use the Information Revealed Without the Consent of the Other Lawyer or Party."

c. "Scrubbing" Metadata to Remove It From Documents
    i. What is "Scrubbing"?
        1. "Scrubbing" is the Process of Removing Metadata From Documents

    ii. May Attorneys Scrub Documents? Yes…If Not Produced Under Discovery
        1. North Carolina State Bar Ethics Committee 2009 Formal Ethics Opinion 1
            a. "Lawyers Have Several Options to Minimize the Risk of Disclosing Confidential Information in an Electronic Communication. Lawyers Should Exercise Care in Using Software Features That Track Changes, Record Notes, Allow "Fast Saves," or Save Different Versions, as These Features Increase the Amount of Metadata Within a Document. Metadata "Scrubber" Applications Remove Embedded

Information From an Electronic Document and May Be Used to Remove Metadata Before Sending an Electronic Document to Opposing Counsel. Finally, Lawyers May Opt to Use an Electric Document Type That Does Not Contact as Much Metadata, Such as the Portable Document Format (PDF), or May Opt to Use Hard Copy or Fax. Both Commercial and Freeware Software Solutions Exist to Help Lawyers Avoid Inadvertently Disclosing Confidential Information in an Electronic Communication."

2. American Bar Association – John Rouse (Feb. 2011)
    a. "Scrubbing Metadata From Documents Produced in Discovery, Particularly When the Metadata is Requested to Be Produced and is Potentially Relevant, is Probably a Violation of the…Federal Rules, and…Will Expose Both the Attorney and the Client to potentially Severe Sanctions."

d. Producing Responsive, Non-Privileged ESI With Appropriate Metadata and OCR (Optical Character Recognition) Extension
    i. Responsibility
        1. Attorneys and Their Clients Have an Obligation to Preserve ESI. Attorneys Must Advise Their Client's That They Must Make a Reasonable Effort to Preserve All Potentially Relevant Information and to Collect and Preserve Data in a Way That is Legally Defensible and Prevents spoliation.

    ii. How to Produce Responsive, Non-Privileged ESI With Appropriate Metadata and OCR
        1. Compress Data to a ZIP or RAR Tool
            a. Reasons

i. This Allows a Clear Data File Size to Be Identified So That a Complete Upload Can Be Verified

ii. This Captures the Metadata of the Original Documents and Allows Copying and Extraction Without Spoliation

2. Preserve, Collect and Process ESI Efficiently With a Litigation Response Plan (see www.edrm.net LRP)

a. Collect, Assimilate, and Document Existing Legal Strategies, Corporate Infrastructure and Topographies, and Electronic Evidence Production Methodologies;

b. Work With the Inside Counsel, Outside Counsel Team, the Corporate Information Technology Team and Records Management Department to Provide Legal and Technical Strategy, Including Data Gathering Strategies, Pleadings, and Best Practices Consultation;

c. Establish a Written Policy to Follow Upon Receipt of a Discovery Request, Preservation Order or Other Similar Item;

d. Ensure That the Company Meets its Legal Obligations While Minimizing the Electronic Discovery Expense and Burden; and

e. Ensure That the Third-Party Consultant Can Provide Expert Witness Testimony in the Event the Implementations of the Electronic Discovery Strategies Come Into Question.

e. Case Law

i. *Zubulake v. UBS Warburg, LLC*., No. 1:02cv1243 (S.D.N.Y. Feb. 15, 2002)

F. WORKING WITH AND SUBPOENAING SOCIAL MEDIA COMPANIES

a. Electronic Communications Privacy Act ("ECPA") 18 U.S.C. § 2510 et seq.

b. Stored Communications Act ("SCA") – 18 U.S.C. § 2701 et seq.

   i. Discusses the Voluntary and Compelled Disclosure of Stored Wire and Electronic Communication and Transactional Records Held By Third-Party Internet Service Providers

   ii. As a General Rule, it is Unlawful For a Provider of an Electronic Communication Service to Knowingly Divulge the Contents of Any Communication While in Electronic Storage By That Service to Any Person other Than the Addressee or Intended Recipient

      1. Lawful Consent: An Electronic Communications Service Provider Can Divulge the Contents of a Stored Communication if it Has Lawful Consent of the Originator or an Addressee or Intended Recipient of Such Communication, or the Subscriber of the Electronic Communication Service.

c. Are Social Media Accounts Covered Under the ECPA or SCA? Yes

   i. Non-Public Social Media Posts, Which Are Intended to Be Private, Are Covered by the SCA Because They Are:

      1. Electronic Communications;
         a. Electronic Communication = Any Transfer of Signs, Signals, Writing, Images, Sounds, Data, or Intelligence of Any Nature Transmitted in Whole or in Part by a Wire, Radio, Electromagnetic, Photo-Electronic or Photo-Optical System (18 U.S.C. § 2510(12))

2. Transmitted Via an Electronic Communication Service;
    a. Electronic Communication Service = Any Service Which Provides to Users Thereof the Ability to Send or Receive Wire or Electronic Communications (18 U.S.C. § 2510(15))

3. In Electronic Storage; and
    a. Electronic Storage: Storage of Such Communication By an Electronic Communication Service For Purposes of Backup Protection of Such Communication (18 U.S.C. § 2510(17)(B))

4. Not Accessible to the General Public
    a. Configured to Be Private = The Statute's Purpose is to Protect Information That the Transmitter Took Steps to Keep Private (18 U.S.C. § 2511(2)(g)(i))

d. Subpoena Exceptions to the ECPA & SCA
    i. Criminal Subpoenas
        1. Enforceable: A Governmental Entity May Require the Disclosure by a Provider of Electronic Communication Service of the Contents of a Wire or Electronic Communication Pursuant to a Warrant

            a. Also Note: A Federal Count May Not Issue a Criminal Warrant Ordering a U.S. Company to Produce Electronic Communications Stored Outside of the U.S.

    ii. Civil Subpoenas
        1. Not Enforceable: There is No Civil Subpoena Exception to the SCA for Contents of Communication

            a. Also Note: "Contents"

i. The SCA States That "Contents" Refers to the Message Conveyed in the Communication, But Not Customer Information Such as the Date, Time, Originating and Receiving Telephone Number for Phone Calls and Text Messages. Non-Content Information May Be Obtained By Litigant

e. Case Law
   i. *Ehling v. Monmouth-Ocean Hospital Service Corp*., 961 F. Supp. 2d 659 (2013)
   ii. *Konop v. Hawaiian Airlines Inc.,* 302 F.3d 868 (2002)
   iii. *Crispin v. Christian Audigier Inc*., 717 F.Supp.2d 965 (2010)
   iv. *Viacom Int'l Inc. v. YouTube Inc.,* 253 F.R.D. 256 (2008)
   v. *Microsoft v. United States*, 2016 WL 3770059 (2016)
   vi. *In Re Subpoena Duces Tecum to AOL, LLC*., 550 F.Supp.2d 606 (E.D. Va. 2008)
   vii. *Mintz v. Mark Bartelstein & Assocs., Inc.*, 885 F.Supp.2d 987
f. Practice Tips
   i. Civil - Narrowly Focus Your Request
      1. "Reasonably Calculated to Lead to the Discovery of Admissible Evidence"
         a. North Carolina Rules of Civil Procedure – Rule 26(b)(1)

   ii. Criminal - View Each Social Media Entity's Law Enforcement Information
      1. Facebook - https://www.facebook.com/help/473784375984502
      2. Instagram - https://help.instagram.com/494561080557017/
      3. Twitter - https://support.twitter.com/articles/41949#8
      4. LinkedIn - https://www.linkedin.com/legal/privacy-policy
      5. Tumblr - https://www.tumblr.com/docs/en/law_enforcement
      6. Snapchat - https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf

G. FACEBOOK'S ARCHIVE FEATURE

a. Facebook Allows Its Users to Download Their Information From The Website Using the Archive Feature

i. Visit the "Download Your Info" Page on Facebook.Com

1. How Can I Download My Information From Facebook?

a. Click Down Arrow At the Top Right of Any Facebook Page and Select Settings

b. Click Download a Copy of Your Facebook Data Below Your General Account Settings

c. Click Start My Archive

2. Can I Pick and Choose Which Information I Would Like to Download?

a. No. The Data File Must Be Downloaded In Its Entirety

3. What Security Measures Are in Place to Make Sure Someone Else Doesn't Download a Copy of My Information?

a. Identity Confirmation

b. Link to Download File is Sent to Account Email Address Only

c. Link to Downlosd File Expires Within a Few Days

d. Password Entry is Required to Download File

e. Download on a Shared Computer My Require Additional Steps

b. What Can Be Downloaded?

i. Data Regarding the User's Account and Activity Log

1. Data Categories List

About Me - Account Status History - Active Sessions - Ads Clicked – Address - Ad Topics - Alternate Name – Apps - Birthday Visibility – Chat - Check-Ins – Connections - Credit Cards – Currency - Current City - Date of Birth - Deleted Friends – Education – Emails - Events - Downloaded Info - Facial Recognition Data – Family - Favorite Quotes – Followers – Following - Friend Requests – Friends – Gender – Groups -

Hidden from News Feed – Hometown - IP Addresses - Last Location - Likes on Others' Posts - Likes on Your Posts - Likes on Other Sites - Linked Accounts – Locale – Logins – Logouts – Messages – Name - Name Changes – Networks – Notes - Notification Settings – Pages - Pending Friend Requests - Phone Numbers – Photos - Photos Metadata - Physical Tokens – Pokes - Political Views - Posts by You - Posts by Others - Posts to Others - Privacy Settings - Recent Activities - Registration Date - Religious Views - Removed Friends - Screen Names – Searches – Shares - Spoken Languages - Status Updates - Work - Vanity URL - Videos

c. What Cannot Be Downloaded?
    i. Any Deleted Information

d. Practice Tips
    i. Utilize the "Download Your Info" Link
        1. https://www.facebook.com/help/131112897028467

H. USING FRIENDING/FOLLOWING TO OBTAIN INFO

a. Friending and Following Explained
    i. Friending is the Act of Adding Someone to a List of "Friends" on a Social Networking Service. Friending Allows the Individuals to Share Information Between Them.
    ii. Following is More Likened to a "Fan" in That a Follower Only Receives Information From the Individual That They Follow.

b. Friending and Following As a Means to Obtain Information
    i. Can the Attorney Friend/Follow?
        1. Friend? No.

a. Friend Request From Fake Account
    i. NCRPC Rule 8.4 Prohibits an Attorney From Engaging in Deceitful Conduct. Therefore, Sending a Friend Request From a Dummy Account or Through a Third Party Would Raise Ethical Concerns.
b. Friend Request From Real Account:
    i. NCRPC Rules 4.2 and 4.3 Limit an Attorney's Ability to Interact with Third Parties Who Are Represented By Counsel or Who May Be Adverse to Their Client's Interests. Therefore, These Rules Would Prohibit an Attorney From "Friending" a Represented Party.
        1. What About Unrepresented Parties? No Clear Guidance. It Would Be Best to Avoid This Behavior To Prevent Any Allegations of Misconduct.

2. Follow? Maybe.
    a. Facebook Following vs. Instagram Following
        i. As a General Rule, All Public Posts are Fair Game For Viewing By Attorneys Because They Are Available to Be Viewed By Anyone Who Has the Ability to View the Posts. However, the Term "Follow" Differs From Site to Site.

    b. Example:
        1. Facebook Following = Fan Type Interaction
        2. Instagram Following = Friend or Fan Type Interaction as Instagram Users Can Limit the Ability to Follow By Request or Leave Following Open to the Public

ii. Can the Client Friend/Follow?

1. Friend? Yes.

a. The Ethical Bar Prohibiting a Lawyer or His or Her Agent From Contacting a Represented Non-Client Does Not Extend to the Client of the Lawyer or the Client's Investigator or Other Agent

2. Follow? Yes

a. As Stated Above, Viewing of Public Information is Permissible

c. Obtaining Information Without Friending or Following

i. There Are No Ethical Implications of Accessing Information That is Freely Available to the Public.

d. Social Media "Scrubbing"

i. Attorneys May Not Advise Their Clients to Delete Social Media Posts As It May Be Seen as Spoliation And Can Result in Sanctions

e. Case Law

i. *Allied Concrete Co. v. Lester*, 736 SE2d 699 (2013)

ii. *Gatto v. United Airlines, Inc.*, 2013 U.S. Dist. LEXIS 41909 (D.N.J. Mar. 25, 2013)

f. <u>Practice Tips</u>

i. NCRPC Rule 1.1

1. The Competency Component Requires That You Advise and Counsel Your Clients on the Potential Legal Impact of Their Social Media Activity.

ii. Do Not Advise a Client to Delete an Existing Post or Otherwise Fail to Preserve Copies of Social Media Posts for Discovery Purposes.

I. WHAT CAN BE DONE IF THE ACCOUNT IS CLOSED?

a. Closed Account vs. Deleted Account

i. Closed Account

1. Follow the Procedures of the ECS

a. Many Closed Accounts Can Be Simply Re-Activated

b. Some ECSs Delete the Data of Closed Accounts

ii. Deleted Account

1. Deleted E-Data is Discoverable Under NCRCP Rule 34

2. *See* Deleted Data Recovery Steps Below

J. OBTAINING DELETED DATA

a. Can Deleted Data Be Recovered? Yes (Sometimes)

i. Obtaining Deleted Data Yourself

1. Directly From the Electronic Communication Source

2. Directly From the Other Party to the Litigation

a. In Discovery Pursuant to NCRCP Rule 34

ii. Hiring a Data Recovery Professional

1. Data Recovery Professionals Are Able to Retrieve Deleted Data From Hard Drives Not ECSs

a. Effectiveness of Data Recovery Professional Depends on the Condition of the Hard Drive

K. PROCESSING, REVIEW AND PRODUCTION PITFALLS

a. Pitfalls and Practice Tips (MN State Bar Association)

i. Failing to Conduct a "Reasonable Inquiry" Regarding ESI

1. Practice Tip

a. To Avoid Sanctions, Attorneys Must Make a Reasonable Inquiry and Properly Supervise Their Clients' Production of ESI (*Qualcomm Inc.* and *GTFM, Inc*.)

ii. Relying Upon Improperly Designed or Executed Keyword Searches

1. Practice Tip

a. Not All Keyword Searches Are Created Equal. To Prevent Waiver of Attorney Client Privilege By Inadvertently Producing Documents, Attorneys Should Carefully Test and Examine the Accuracy of Any Keyword Protocol, Particularly in Regard to the Screening of Privileged Documents. (*Victor Stanley, Inc*.)

iii. Exposing Confidential Information to "Metadata Miners"

1. Practice Tip

a. Attorneys Should Exercise Caution When Sharing Electronic Documents and Take Steps to Minimize or Eliminate Metadata in Documents Shared Outside of the Discovery Context (*Madison River Mgmt. Co*.)

iv. Failing to Disclose the Receipt of Inadvertently Produced Documents

1. Practice Tip

a. A Lawyer Who Receives a Writing Relating to the Representation of the Lawyer's Client and Knows or Reasonably Should Know That the Writing Was Inadvertently Sent Shall Promptly Notify the Sender. (NCRPC Rule 4.4) (*Jones*)

b. Case Law

i. *Qualcomm Inc. v. Broadcom Corp*., No. 05-1958, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008)

ii. *GTFM, Inc. v. Wal-Mart Stores, Inc.*, No. 98-7724, 2000 WL 335558 (S.D.N.Y. Mar. 30, 2000)

iii. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D. Md. 2008)

iv. *Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp*., 387 F. Supp. 2d 521 (M.D.N.C. 2005)

v. *Jones v. Eagle-North Hills Shopping Centre, L.P*., 239 F.R.D. 684 (E.D. Okla. 2007)

What to Do with It: Processing, Review and Production

Submitted by Corey V. Parton

Now I have the Data, Now What?

Organize Chronologically.

Don't organize by type (emails, text messages etc.)

Allows the ESI to serve as a reference to the narrative already presented by your client.

Easy redaction of evidence based on value later on.

When dealing with emails, include entire chain for each email, even though it will be redundant.

Reviewing the Data

Read Everything

Thoroughly, twice and with an open mind. Some attorneys tend to search discovery for corroborative facts.

Look for "Zebras" First

Most ESI discovery will lead to information that will require the discovery of additional evidence, such as deleted emails, the other side of a social media conversation, documents referenced in the ESI etc.

Large, unnatural gaps in communications.

ESI that infers the author's knowledge of information they would not have had access to at the time of the ESI's creation.

Communication that seems unnatural to the parties or outside of the conversational "flow".

Existence of important documents, witnesses or communications that can be obtained with supplemental discovery.

ESI that differs unnaturally from that same ESI's current form.

Rate by Degree of Helpfulness/Harm to Client

Doing so first will allow you to make appropriate decisions on whether to object or assert a privilege when producing ESI.

Also looking for additional claims that may be added with leave of court. The quicker the better. *See* N.C. Gen. Stat. § 1A-1, Rule 15.

Citing Online Content Properly

Columbia Law Rev. Editors et. al.,The Bluebook, R. 18.2.1-2 (20th ed. 2016).

Not generally done in discovery production.

Only needed for submissions to the court.

Processing the Data

Rule 1006

Have your client create summaries or other organizational documents emphasizing helpful facts in the ESI that may be admissible later. *See* N.C. Gen. Stat. § 8C-1, Rule 1006.

Dictate the Form Early

The requesting party "specify the form or forms in which electronically stored information is to be produced." N.C. Gen. Stat. § 1A-1, Rule 34(b). However, the

responding party may state an objection to a requested form for producing electronically stored information but they then must stat the form they intend to use. Id.

By processing the ESI early on in a reasonable form, you may have better grounds to object to a more burdensome or costly form specified by the requesting party.

Testing ESI, Including Comparison, Hash Tags, Encryption & Metadata

Hashtag

A word or phrase preceded by a "#" used within a message to identify a keyword or topic of interest and facilitate a search for it. Basically a user generated key-word that their post will be associated with and searchable by.

"Trending topics"

So by conducting a search using the hashtag contained in the ESI, you may be able to find related content from other users of the same social media forum.

Metadata

Data that describes the "characteristics" of ESI and can describe things like how, when and by whom the ESI was created, modified, accessed etc. The Sedona Conference

Glossary: E-Discovery & Digital Information Management 2nd Ed. (Dec. 2007). An example would be a .doc on Dropbox. Metadata would tell you who created, edited, modified or saved the document and when.

May be saved in multiple locations, such as on Dropbox and an individual users laptop.

Metadata can be used to verify the document like you would any other piece of evidence. If you suspect a document was created after the time it was purported to be, a supplemental discovery response for the documents metadata may be determinative.

Conflicting metadata may indicate intentional modification of the ESI.

Encryption

Determination as to its necessity is required in some circumstances such as discovery of ESI in Federal criminal cases. *See* Dep't. of Justice et. al., Strategies and Commentary on ESI Discovery in Fed. Crim. Cases, ¶5.p.ii (Feb. 2012).

Contact Comparison

With social media, use followers, friends etc. to verify the content via their media feed. With emails and messages, investigate the "other side" of the conversation to ensure it is accurate. This will also aid with admissibility down the road.

Investigate email and notification settings of social media and then investigate whether those notifications or emails were ever actually generated by the social media application. Added benefit is you have made another individuals emails potentially discoverable.

Cell phone store employee to provide verification of text messages. *See* State v. Taylor, 187 N.C.App. 395, 413 (2006).

Producing Responsive, Non-Privileged ESI with Appropriate Metadata and OCR

Generally Discoverable

ESI is generally discoverable like all other types of evidence so long as it is reasonably calculated to lead to the discovery of relevant evidence. N.C. Gen. Stat. § 1A-1, Rule 26(b)(1). However, ESI is also subject to the limitations contained in Rule 34(b), and any other conditions the Court specifies. Id. Rule 26(b)(1b).

Metadata

"ESI" includes *reasonably accessible* metadata that will enable the discovering party to have the ability to access such information as the date sent/received, author, and recipient. N.C. Gen. Stat. § 1A-1, Rule 26(b)(1) The phrase does not include other

metadata unless the parties agree otherwise or the court orders otherwise upon a showing of good cause. Id.

Compare Analog Devices, Inc. v. Michalski et. al., 2006 NCBC 14 (N.C. Super. Ct. Nov. 1, 2006); Bank of America Corp. v. SR international, Inc., 2006 NCBC 15 (N.C. Super. Ct. Nov. 1, 2006).

Courts seem unwilling to impose the burden and cost of having to hire an outside "recovery team" to produce ESI that was destroyed in good faith.

Discovery Conferences

Attorneys "may request a meeting on the subject of discovery, including the discovery of electronically stored information" any time 40 days after filing of a complaint. N.C. Gen. Stat. § 1A-1, Rule 26(f)(1). The opposing party is then obligated to meet within 21 days and a discovery plan must be submitted to the court within 14 days if one is agreed upon. Id. Rule 26(f)(1)-(3).

A good faith conferencing attempt may also be prerequisite to a motion asking the court to allocate the costs of ESI discovery. *See* Id. Rule 26(f)(4).

Failure to participate in good faith can also result in an award of attorney fees. Id. Rule 37(g).

Participation in a discovery agreement likely does not constitute a waiver of client's right assert privileges or objections. *cf.* Morris v. Scenera Research, LLC, 2011 WL 3808544 (N.C. Super. Aug. 26, 2011).

Enforcement

If a requesting party moves for a Court Order compelling the production of ESI, the burden shifts to the producing party to show the basis for its objection. N.C. Gen. Stat. § 1A-1, Rule 37(a)(2). The Court is then required to award reasonable expenses if the requesting party's motion is granted, unless the Court finds the opposition was substantially justified. Id. Rule 37(a)(4).

Safe Harbor

Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system. N.C. Gen. Stat. § 1A-1, Rule 37(b1).

Clients not anticipating litigation may need to be advised to adopt a policy of routinely destroying ESI after a specified period of time.

Privilege Logs

Required when withholding information *otherwise discoverable* by claiming a privilege.

Withheld Information	**Format/Type**	**Privilege Asserted**	**Basis for Assertion**

Must be done in a manner that allows the other party to assess the privilege claim. N.C. Gen. Stat. § 1A-1, Rule 26(b)(5)(a.). The privilege claim may be asserted after an inadvertent disclosure. Id. Rule 26(b)(5)(b.).

Protective orders can be used to ensure confidential, non-privilege information remains protected. Id. Rule 26(c).

How to Get it Authenticated and Admitted

Submitted by Corey V. Parton

Proactively Ensuring Authenticity.

Authenticity is a subset of relevancy, so when we talk about authenticity we are really talking about admissibility down the road.

Tools

By using Requests for Admissions you can ensure authenticity of disputed documents as well as ensure admissibility early on. N.C. Gen. Stat. § 1A-1, Rule 36; *See* N.C. Gen. Stat. § 8C-1, Rule 1008.

Sample:

1. Admit that you sent an email to Jane Doe on December 31, 2016.

2. Admit that you sent an email to Jane Doe on December 31, 2016, that contained the following text: "Dear Mrs. Doe…."

3. Admit that a true and accurate copy of the email you sent to Jane Doe on December 31, 2016 is attached hereto as "Exhibit 1".

By using Interrogatories, you can identify all corresponding accounts or information that can be used for comparison and verification. N.C. Gen. Stat. § 1A-1, Rule 33.

Sample:

1. Identify all social media accounts that Defendant accessed between July and November of 2017, including the unique identifier such as the username, "handle" or account login name.

2. Identify all IP addresses Defendant used to access the above referenced accounts on more than one occasion between July and November of 2017.

3. Identify all of the electronic mail accounts you sent or received emails from between July and November of 2017.

4. Identify the Company's policy for retention of electronic mail, including whether it is archived or deleted and after what time frame.

Through Depositions you can authenticate the documents or identify other important details. N.C. Gen. Stat. § 1A-1, Rule 30, Rule 31, Rule 32.

Subpoena records from cell phone or social media companies. N.C. Gen. Stat. § 1A-1, Rule 45.

Waiver by the Opposing Party. One creative idea may be to send a letter informing Opposing Counsel that you believe them to be in possession of an original document of which you have a copy, and that the contents would be a subject of proof at the hearing. If they do not produce the original at the hearing, you may be entitled to admit the duplicate. *See* N.C. Gen. Stat. § 8C-1, Rule 1004(3).

An Affidavit from your own client with the ESI attached as an exhibit, if submitted in support of a pre-trial motion, creates additional corroborating evidence of authenticity, and may, theoretically, make the ESI part of the court file and potentially admissible as a public record. N.C. Gen. Stat. § 8C-1, Rule 902(4).

Testimony. This seems obvious, but it is sometimes overlooked. *See* United States v. Drew, 2009 WL 2872855 (C.D. Cal Aug. 28, 209) (unpublished).

Has the ESI Changed? What Evidence is Need to Prove it Hasn't?

Registry Files obtained through discovery can offer insight into whether or not a computer has been tampered with and when.

Documentation proving chain of custody of the ESI can be obtained through discovery.

Protocol specifying the storage methods and means of the original ESI and how it should be transferred format-wise for production, can be agreed upon with Opposing Counsel. *See* N.C. Gen. Stat. § 1A-1, Rule 26(f)(1), Rule 34(b).

Chain of Custody should only include qualified individuals with experience or expertise in transferring or handling ESI.

If you are the objecting party you can use the chain of custody to sow doubt as to the authenticity of the ESI by showing the admitting party's inability to rule out what could have happened, since ESI can change quickly and drastically.

How to Prove Electronic Documents Have Not Been Modified.

Metadata should not have been changed since the preservation of the evidence.

Electronic Data Recovery Companies can assist with the gathering and analysis of ESI. ***Pro-tip:*** Get a quote and time estimate early on so you have a good faith basis for objecting to the production of discovery based on undue hardship. North Carolina Courts have been reluctant to force parties, regardless of assets, to pay large sums of money to data recovery companies in order to produce ESI. *Compare* Analog Devices, Inc. v. Michalski et. al., 2006 NCBC 14 (N.C. Super. Ct. Nov. 1, 2006); Bank of America Corp. v. SR international, Inc., 2006 NCBC 15 (N.C. Super. Ct. Nov. 1, 2006).

Identifying Who Made the Post and Linking to the Purported Author.

Authentication in the ESI context refers to whether the alleged author actually made the ESI. North Carolina's standard for authenticity is low, and courts have held that questions about accuracy generally go to the weight, not the admissibility of the information. *See* Horne v. Vassey, 157 N.C. App. 681 (2003). Still, in order for a piece of ESI to be relevant it most be linked to the person purported to have made it. *See* U.S. v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992); N.C.R. Evid. 104 commentary. Keep in mind that relevancy limits still apply.

Is the Evidence What the Proponent Claims?

If the ESI is being admitted to prove the truth of its contents, then the Original Writing Rule applies as it would to any other document. *See* N.C. Gen. Stat. § 8C-1, Rule 1001(1). However, North Carolina generally will allow duplicates unless there is a genuine issue as to its authenticity. *See* N.C. Gen. Stat. § 8C-1, Rule 1003.

Does the ESI Have Distinctive Characteristics?

Authenticity must be shown through other admissible evidence, but it does not necessarily have to be direct evidence. *See* N.C. Gen. Stat. § 8C-1, Rule 104(b), Rule

901(a). The circumstantial evidence used to prove authenticity may include "distinctive characteristics". *See* N.C. Gen. Stat. § 8C-1, Rule 901(b)(4); State v. Taylor, 178 N.C. App. 395 (2006).

Examination of Circumstantial Evidence.

The fact that the ESI contains the purported author's name, biographic information or photograph (think signature line on an email, or Facebook profile page printout) will generally not be sufficient by itself because it is so easy to falsely generate that type of ESI. Some additional corroborating characteristics and circumstances may include:

Intimate Information that only the sender could know, such as a nickname or intimate details about the sender's relationship with the recipient. *See* State v. Williams, 191 N.C. App. 254 (2008).

Sender self-identifying in the post itself (think Jon Gotti). *See* State v. Taylor, 178 N.C. App. 395 (2006).

Corroborating conduct by the sender, such as a post indicating an intention to participate in a protest followed by the sender's arrest at that same protest.

Metadata may, for example, indicate that the company's dropbox indicated that John Doe altered or created the document at a certain time; followed by witness evidence that John Doe was present and at his computer at approximately that time.

Internet History

Show the Source, such as a social media company that keeps a record of the name or email address associated with that account and required additional information at the time the person registered with the social media site.

State Interpretation of Federal Rule 901.

North Carolina's Rule 901 is identical to Federal Rule 901. N.C. Gen. Stat. § 8C-1, Rule 901, commentary.

Proven Methods for Testing ESI.

Identifying untimely changes in Metadata.

Proving computer tampering through Registry Files.

Challenging deficiencies in Chain of Custody.

Attacking Authenticity.

Self-Authentication Methods

Rule 902 provides a number of scenarios where ESI may be self-authenticated without independent, admissible evidence. N.C. Gen. Stat. § 8C-1, Rule 902.

This may also be done early on by Affidavit, if your client was the recipient or originator of the ESI, or by Stipulation with Opposing Counsel.

Real Life Examples and Recent Case Law

Instagram vacation photos.

Company group chat.

Five years worth of copies of checks.

Changing microchip.

Disappearing surveillance video.

Legal Ethics and ESI

Submitted by Brian W. King

LEGAL ETHICS AND ESI

3:30 – 4:30

BRIAN W. KING

Think about what people are doing on Facebook today. They're keeping up with their friends and family, but they're also building an image and identity for themselves, which in a sense is their brand. They're connecting with the audience that they want to connect to. It's almost a disadvantage if you're not on it now. Mark Zuckerburg.

The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency. Bill Gates

Technology can be our best friend, and technology can also be the biggest party pooper of our lives. It interrupts our own story, interrupts our ability to have a thought or a daydream, to imagine something wonderful, because we're too busy bridging the walk from the cafeteria back to the office on the cell phone. Steven Spielberg

We drift through the day, everyday, using technology unlike any generation before us. I can tell you, with a few simple clicks of buttons what I did exactly ten years ago. Where I was, who I met with, and why I met with them. I can probably do the same with most of the people in this room with a few simple clicks.

Technology has modified our lives, but it has also modified our ethics. What we are now, and who we are now are not the same.

I want to thank Kate Rech for her work on this topic in 2016. This work is simply a revision and update of her work. Kate is a fantastic family law attorney in Charlotte, on the front lines of this battle we all wage.

Ethics in Obtaining ESI

A. Client Confidentiality and Competent Representation: What Does it Really Mean?

ESI is Electronically Stored Information. That may no longer be a good way to describe what actually happens with data, as there is no vault of information that can be opened, easily packaged, modified or destroyed. It is in everything that we do. Where we are, where we have been, what we have done, and virtually every other part of who we are is stuck somewhere in ESI.

Family Law is particularly stuck in ESI, as the information we seek is not necessarily contained in neatly drafted documents or a series of contracts. Instead, it is scattered across people's lives.

Perhaps the criminal lawyer will argue that the age of hiding is over, and the cast of light has changed their practice more, or even the transactional attorney will immediately point on how data is transferred has revolutionized that practice—but I would argue that today it is the family lawyer whose life has drastically changed the most. Real time impressions on anything are readily available, and often drafted directly by the person impacted. Where your client was at any given time is a mere subpoena away.

Obviously when it comes to ethics, the lawyer has many issues to concern with. The first is confidentiality.

North Carolina Rule of Professional Conduct 1.6(c), a lawyer must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information to the representation of a client"

This is a duty to be placed on attorneys, which demands for us to take special efforts to prevent mistakes when sending confidential client information, including ESI. This is a responsibility placed on the lawyer, not the client.

There are alternative rules in place in the event a disclosure of information occurs. Federal Rule of Evidence 502(b), disclosure of privileged material will not constitute waiver of the privilege if these three criteria are met: (1) where the disclosure was inadvertent; (2) where the person holding the privilege took reasonable steps to prevent disclosure; and (3) where the privilege-holder took prompt and "reasonable steps to rectify the error".

What are these reasonable steps? First, it is important that email to the client is carefully kept confidential. Next, that there is an aggressive mechanism in place to make sure if there is a mistake, that that mistake is immediate in its attempt to resolve.

Rule 26(b)(5)(B) of the Rules of Civil Procedure details what must be done following inadvertent disclosure.

In the event there is a disclosure by mistake, the disclosing party immediately notifies the receiving party of a mistake, and the receiving party must promptly return, sequester, or destroy the specified information as well as any copies.

Moreover, the receiving party cannot use or disclose the protected information until the claim is resolved. If this party already disclosed this information, it must take

reasonable steps to retrieve the information. However, the receiving party may also deliver the information to the court under seal so that a judge may decide the claim.

If the parties wish to take matters into their own hands, they may negotiate and execute a non-waiver agreement or "clawback" agreement in lieu of simply relyingon the rules. Such agreements are usually negotiated at the beginning of a case, before any inadvertent disclosures may tempt one party of the other to improperly use the mistakenly discovered information.

This may seem drastic, but I recently had a case in which this applied. We had arguments between partners at a psychological group that led to a breakdown of the partnership. In the middle laid thousands of paper and electronic files of confidential information. We meticulously put together agreements that allowed each partner access to files, dates and times, and what to do with files to make sure none of these files landed in the wrong hands.

For attorneys you work with commonly, or for DSS records, there should be a clear agreement on how and when to use this documentation.

These agreements will anticipate inadvertent disclosures, mitigating risks to both parties, and outlines the responsibilities upon such disclosures.

These agreements must include the non-waiver provision, that protects the inadvertent disclosure does not constitute a waiver of the attorney-client privilege.

B. Client Confidentiality and Social Media

Many individuals going through a divorce freely text, email and status-update without considering the strategic risks and dangers that come along with these types of electronic communications. Before you post your next Facebook update, consider some interesting stats from the American Academy of Matrimonial Lawyers[1]

These statistics are from the American Academy of Matrimonial Lawyers:

- 92% of AAML divorce attorneys cited an increase in cases using **evidence taken from smart phones** during the past three years.

- In the same survey, 94% noted an increase in **text message evidence**.

[1]http://www.aaml.org/about-the-academy/press/press-releases/divorce/lawyers-finding-divorce-app-smart-phones

: http://family-law.freeadvice.com/family-law/divorce_law/emails-in-divorce-proceedings.htm#ixzz4Qw9Xalj9

- 81% of AAML members say they have seen increased use of **evidence from social networking websites** during the past five years (with Facebook being cited as the primary culprit).

There is little doubt as to why this topic is so timely, all studies and advocacy groups have spoken in unison: Electronic communication is on the rise, and will continue to increase.

Interestingly, the AAML has said, "This rise in the use of electronic evidence, however, generally has not been lamented by divorce attorneys. In fact, it has made our jobs easier by providing a virtual treasure chest of potential exhibits and evidence for trial. Therefore, in all likelihood, if you choose to use electronic communication during your divorce, you may have to explain it in court."[2]

Free Advice Legal "Given this state of affairs, it advisable for any spouse going through a divorce proceeding to consider the following general principles before sending any electronic communication - because once you hit the send, post, or tweet button, it is permanently backed up and accessible to your spouse and their attorney. The following is advised to all family law clients. This list is a good checklist of things you may want to share with each and every client in the family law area:

Presume that every communication will be entered into evidence, and only include language or information that you would like your judge to see. Let's be real, clients are going to talk freely, and they are not in the emotional best state when going through a divorce. However, I think this hard line position makes a lot of sense from the beginning.

Don't send any text message, Facebook status update, or e-mail in a moment of anger. These can be taken out of context in divorce proceedings and used to paint an untrue and unflattering picture of your personality. This advice makes sense, but telling clients what to do during anger is difficult at best.

Prepare a first draft of any e-mail concerning the divorce (or that will be sent to your spouse) and review it to ensure that it accurately conveys your intentions and demeanor and cannot be misinterpreted.

I personally remember a case where the other side did not have a Facebook account, but his girlfriend did—and he had no idea. I arranged the photos where he

[2] https://www.mckinleyirvin.com/Family-Law-Blog/2013/September/The-Hazards-of-Email-Text-Messages-038-Social-Me.aspx

would continue to deny all the things her "new sugardaddy" had purchased, finally ending with a picture of her and him at an event at Myrtle Beach.

Courts in general are not apt to protect those who have posted photographs and words in Social Media. Courts have often concluded that there is no reasonable expectation of privacy on social networking sites at all.

Some of the most common ways that emails and texts come in as admissible evidence are:

- To indicate a person's state of mind
- Identify where a person was at a particular day and time
- Show collaboration between two parties
- Contradict statements made in court or in pre-trial disclosures

In order to use this evidence, you need to learn authentication. The Federal Rules of Evidence require that any piece of evidence (including electronic communications) be authenticated. This is inherently difficult to do when the very nature of email is that it occurs in private—with few markers of authenticity.

- Rule 901. Authenticating or Identifying Evidence
    - **(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.
    - **(b) Examples.** The following are examples only — not a complete list — of evidence that satisfies the requirement:
        - **(1)** ***Testimony of a Witness with Knowledge*****.** Testimony that an item is what it is claimed to be.
        - **(4)** ***Distinctive Characteristics and the Like*****.** The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.
        - **(5)** ***Opinion About a Voice*****.** An opinion identifying a person's voice — whether heard firsthand or through mechanical or electronic transmission or recording — based on hearing the voice at any time under circumstances that connect it with the alleged speaker.

- **(6)** ***Evidence About a Telephone Conversation.*** For a telephone conversation, evidence that a call was made to the number assigned at the time to:
    - **(A)** a particular person, if circumstances, including self-identification, show that the person answering was the one called; or
    - **(B)** a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.

In the case of electronic communications, this generally means that it must be shown that you are the person that actually sent or posted the communication in question.

This can be done by:

1. Having the other side admit sending it.
2. Have the document admitted under a hearsay exception
3. An email may also qualify as a "past recollection recorded." This would require that the email itself may not actually come into evidence, but used as a tool to refresh a witness's faded memory. (Fed. R. Evid. 803(5).)

There will be objections, and even some expert testimony in certain cases, stating that using personal texting as evidence is an invasion of privacy and therefore should not be admissible in court.

One must first find was level of privacy is actually applied: (1) Social Media has little to no expectation of privacy, (2) A joint account for a computer or service would decrease the expectation of privacy.

An important case that clarifies the way the Federal Court system views emails in United States v. Safavian, 435 F. Supp. 2d 36, 39–40 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C. Cir. 2008).)[3] In that case, the Court clarifies that emails are not business records, they are statements that need to be found to be authentic. In that case, the parties had over 460,000 emails that were part of an investigation. In the end, they

[3] *Mark Mermelstein is a Los Angeles–based partner and Christin J. Hill is a San Francisco–based senior associate at Orrick, Herrington & Sutcliffe. Mermelstein also chairs the firm's Cybersecurity and Data Privacy Group.*

found that authentication is a slight burden—not one that has to be over analyzed. The mere showing of an email address was enough to show they appeared to be authentic.

The Court there relied on United States v. Coohey, 11 F.3d 97, 99 (8th Cir. 1993), holding that "the proponent need only demonstrate a rational basis for its claim that the evidence is what the proponent asserts it to be" in order to meet the ground of authenticity. It is clear that the preferred method of authentication is to simply call the person who made the email and find that it was in fact their own work. If not, simply showing that a person received an email and that email has an identifiable address should be enough to reach that level of authenticity.

The work of the attorney begins immediately. Upon retaining a client, you should immediately send a letter requesting for the preservation of all social media accounts, emails and electronic documentation. We call this a spoliation letter, and I have included a copy of the one I use.

You can immediately subpoena the text messages from all numbers by requesting the records from the cell phone provider. This should be done almost immediately.

Judge Michele Lowrance and **Pamela J. Hutul**[4] state, "Cell phones offer other avenues to obtain interesting discovery. Look at a spouse's cell **phone bill**: what are commonly called numbers that are unknown to the family? An inquiry by reverse checking those numbers may tell what other persons or businesses have captivated the time of the spouse when not involved in family affairs (www.freephonetracer.com, eHow.com, and reversemobile.com). This may provide an opportunity to use embarrassing information for marital indiscretions, obsessions or interests that can be useful in managing the case."[5]

Once you have these numbers, you can clearly show that the text apply to these as well. You can do the same for email information. First, ask the person for their information and include any and all email addresses they may use. Later, even if they

[4] Judge Michele Lowrance *was a domestic relations lawyer for twenty years prior to becoming a domestic relations judge in the circuit court of Cook County, Illinois. She is the author of the book The Good Karma Divorce and Pamela J. Hutul is a partner of* Davis Friedman*, a Chicago law firm specializing in family law since 1976. She is certified in Collaborative Law and Mediation and named a Fellow at the Collaborative Law Institute of Illinois.*

[5] http://familylawyermagazine.com/articles/social-media-in-divorce-proceedings

deny the email itself, the document should show that it came from an email that person admitted earlier was used as an email.

You should immediately try to get ahold of any computer in the home. If one party has legal access to the other party's email account, the transmissions sent by the address owner will be evidence admissible in Court.

Finding a Treasure Trove of Information in the Metadata. **Metadata** is "data [information] that provides information about other data".[6] Three distinct types of metadata exist: **structural metadata**, **descriptive metadata**, and **administrative metadata**.[7] Descriptive metadata describes a resource for purposes such as discovery and identification. It can include elements such as title, abstract, author, and keywords.

Structural metadata indicates how compound objects are put together, for example, how pages are ordered to form chapters. Administrative metadata provides information to help manage a resource, such as when and how it was created, file type and other technical information, and who can access it.[8]

Although the Federal Rules of Civil Procedure have only specified rules about electronic documents, subsequent case law has elaborated on the requirement of parties to reveal metadata.[9] In October 2009, the Arizona Supreme Court ruled that metadata records are public record. It is probable that most courts would find this information to be public.[10]

Document metadata have proven particularly important in legal environments in which litigation has requested metadata, which can include sensitive information detrimental to a certain party in court. Using metadata removal tools to "clean" or redact documents can mitigate the risks of unwittingly sending sensitive data. This

---

[6] https://www.merriam-webster.com/dictionary/metadata

[7] *Marcia (2004).* "Metadata Types and Functions". *NISO. Retrieved 5 October 2016.*

[8] *National Information Standards Organization (NISO) (2001).* Understanding Metadata *(PDF). NISO Press. p. 1.* ISBN 1-880124-62-9.

[9] *Gelzer, Reed D. (February 2008).* "Metadata, Law, and the Real World: Slowly, the Three Are Merging". *Journal of AHIMA. American Health Information Management Association.* ***79*** *(2): 56–57, 64. Retrieved 8 January 2010*

[10] *Walsh, Jim (30 October 2009).* "Ariz. Supreme Court rules electronic data is public record". *The Arizona Republic. Phoenix, Arizona. Retrieved 8 January 2010.*

process partially protects law firms from potentially damaging leaking of sensitive data through electronic discovery[11].

There are literally hundreds of websites and applications that are designed to find and restore deleted emails. These sites are so numerous that the service is competitive—and frankly cheap. Many of these sites are specifically to recover old cell phone data, and can pull information from even damaged devices. The work that is done in this field is simply amazing to those of us not technically inclined. It truly is almost scary what is able to be restored. There is some truth to the idea that a computer never truly erases data. It is not uncommon to find emails that have been deleted, trash "cleared" and left on a computer for months or even years.

David Wilkinson in November, 2016 went in detail to explain in his article "4 Steps to Acquiring Text Messages by Subpoena in Divorce Cases".[12] He directly addressed the text message and how to obtain those items. Wilkinson suggests that a cell phone carrier only keeps texts for a period of two or three days. He points out that what is often used to defend against subpoena is the Stored Communications Act, this is all explored later.

There is a four step process, explained by Wilkinson as the following:

1. First, try to get the cell phone company to retain the content of the text messages by **sending a letter** to the carrier explaining that the text messages are evidence and must be preserved. You should site the based provisions of the *Stored Communications Act* and applicable state law. The letter should be sent certified by overnight delivery.

2. Second, **prepare the subpoena** to seek the relevant text message(s).

3. Third, **file an ex parte motion** with your divorce court and request that court order the other party to sign a notarized consent to release the text messages.

4. Fourth, **serve the subpoena**. This may be tricky depending on what state your divorce is being handled, as the rules for service vary from state to state.

---

[11] *Gelzer, Reed D. (February 2008).* "Metadata, Law, and the Real World: Slowly, the Three Are Merging". *Journal of AHIMA. American Health Information Management Association. **79** (2): 56–57, 64.*

[12] http://www.divorcemag.com/blog/acquiring-text-messages-by-subpoena-in-divorce-cases

You may need to have a "commission" set up in the state that the cell carrier's records are kept to ensure the subpoena is properly served.

Obviously, this is a significant amount of work. Fortunately, there are far better options. You may be able to obtain a copy of the text message from the recipient of the message, which you can then print off and produce as evidence at your hearing. You will just have to "lay the foundation" for the message by establishing it was sent by a specific phone number to the recipient's phone

You may be able to obtain a copy of the message from the sender. Try sending a "Demand for Inspection and Production of Documents" to the opposing party, and include a request for copies of the message, or make the opposing party produce his or her cell phone for inspection.

If the sender is not a party to the case, try sending a deposition subpoena and have the person appear at your office for a deposition. That is helpful in some situations, such as domestic abuse cases where one party sends hundreds of text messages to their spouse or significant other to harass or threaten th.

As a practice tip: Download and use iExplorer, a file transfer app, which will help you create printable pages for your text messages.

It is difficult or impossible to subpoena emails from Google and the other companies in the email business. The Federal Law protects these providers with the Federal Stored Communications Act (SCA), 18 U.S.C. § 2702(a)(1), sometime referred to as the SCA.[13] The SCA "prohibits Internet service providers from producing e-mails in response to a civil discovery subpoena," Bellas and Ford write. "As a result, many courts across the United States have quashed subpoenas on the basis that an Internet service provider cannot be compelled to disclose a party's emails pursuant to a civil subpoena."[14]

"Trial lawyers do have an alternative though - a request for production under Rule 34 of the Federal Rules of Civil Procedure, which enables the requester to get the emails directly from the party if the rule's requirements are met 'If an attorney can demonstrate that the e-mails are in the party's possession, custody, or control, then it is

[13] https://www.isba.org/ibj/2015/01/whyyouprobablycan%E2%80%99tsubpoenaemailgoo

[14] George S. Bellas and Steve Ford write in the November 2014 issue of ISBA's *Trial Briefs*.

likely that he or she can obtain them with a request for production,' Bellas and Ford write."

The go on to say, "The Northern District of Illinois is among the courts that have quashed subpoenas under the SCA. "In…*Special Markets Insurance Consultants, Inc., v. Lynch* [2012 WL 156348 (N.D. Ill. 2012)], the plaintiffs had served subpoenas on Yahoo to produce 'the complete e-mail records' of at least three private e-mail addresses owned by the defendants,…Citing a number of federal cases,…the court in *Lynch* quashed the civil subpoena because it violated the SCA."

The ABA has dealt with the authentication of emails directly, as this is more of a national issue, which is quoted from liberally, "Overcoming Authentication and Hearsay Issues in Email Evidence" by Dennis I. Wilenchik and Brian J. Hembd – March 4, 2014.[15] Wilenchik and Hembd believe that too "any attorneys believe emails will be admitted easily or have given little thought to their admissibility. That is a mistake. Emails are actually more susceptible to authentication and hearsay issues than other pieces of evidence."

Below are some basic email authentication and hearsay objections and potential solutions that are important, not only in trial, but also in moving for summary judgment. *See, e.g.*,*Orr v. Bank of Am., NT & SA*, 285 F.3d 764, 773 (9th Cir. 2002) ("A trial court can only consider admissible evidence in ruling on a motion for summary judgment."); *Beyene v. Coleman Sec. Servs., Inc.*, 854 F.2d 1179, 1181 (9th Cir.1988); Fed. R. Civ. P. 56(e).

An email can be self-authenticating. Federal law (and most states following the Federal rule allows documents as self-authenticating when there is "[an] inscription, sign, tag, or label purporting to have been affixed in the course of business and indicating origin, ownership, or control." (Fed. R. Evid. 902(7).)

How to Block the Opposing Party's Retrieval and Admission of Email Evidence. In general, you will know that there are emails that the other side will be introducing into testimony. You know this from discovery, depositions—or even information from your client.

You should begin each trial with a pre-trial order (or at least an informal hearing) where these pieces of evidence are reviewed.

[15] http://apps.americanbar.org/litigation/committees/trialevidence/articles/winter2014-0314-overcoming-authentication-hearsay-issues-email-evidence.html

Each email must begin through the authentication process, and that damage should be done before the trial—when the evidence may already be damning.

In family court, the judge is often the trier of fact—but also serves as the legal gatekeeper. If the evidence is argued before trial, it may allow the judge to set apart that factual evidence in a more clear and concise manner.

THANK YOU

for choosing NBI for your
continuing education needs.

Please visit our website at
www.nbi-sems.com
for a complete list of
upcoming learning opportunities.

NBI | NATIONAL BUSINESS INSTITUTE ™