ESI, E-Discovery & Other Tech Issues for Mediators

(What are these lawyers fighting about?)

chopkins@mcdonaldhopkins.com

Christopher Hopkins

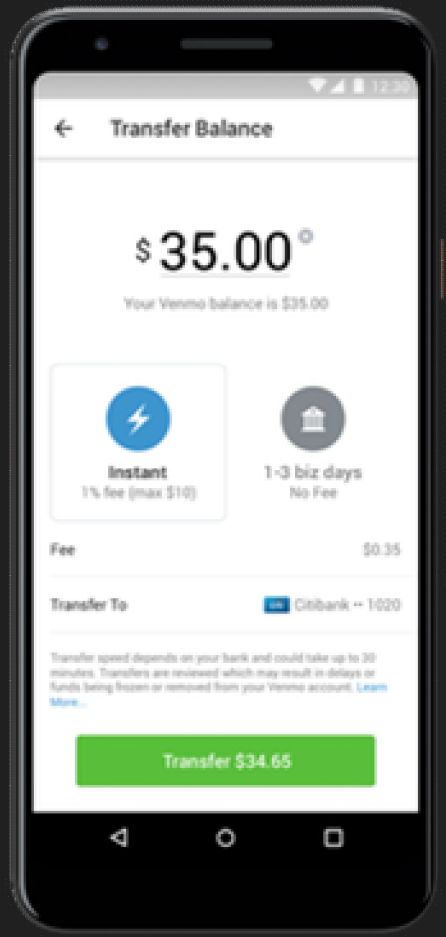
McDonald Hopkins LLC – West Palm Beach

Lawyer, mediator, and arbitrator.

Christopher's practice involves a wide range of emerging technologies including cybersecurity, internet crimes, defamation, privacy, policy drafting, and social media discovery.

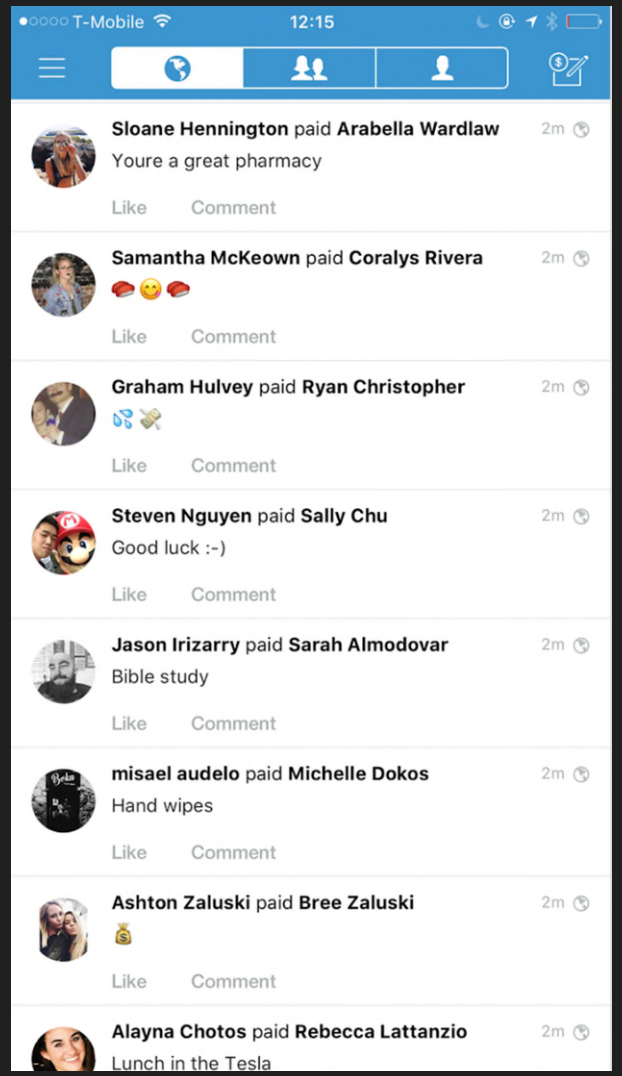
Let’s Get You Paid

McDonald Hopkins



Let’s Get You Paid

McDonald Hopkins



Gaetz Paid Accused Sex Trafficker, Who Then Venmo'd Teen

FOLLOW THE MONEY

When Joel Greenberg made his Venmo payments to three young women, he described the money as being for "Tuition," "School," and "School."

Jose Pagliery Political Investigations Reporter | **Roger Sollenberger** Political Reporter

Updated Apr. 09, 2021 1:00PM ET / Published Apr. 08, 2021 7:39PM ET

EXCLUSIVE

Matthew Louis Gaetz II

Member in Good Standing | Eligible to Practice Law in Florida

Bar Number:	48962
Mail Address:	301 Brooks St SE Fort Walton Beach, FL 32548-7234 Office: **850-897-5405**
Email:	**matt@mattgaetz.com**
Personal Bar URL:	https://www.floridabar.org/mybarprofile/48962
vCard:	
County:	Okaloosa
Circuit:	01
Admitted:	02/06/2008
10-Year Discipline History:	None
Law School:	William & Mary Law School

FLORIDA BAR ETHICS OPINION
PROPOSED ADVISORY OPINION 21-2
March 23, 2021

Advisory ethics opinions are not binding.

A lawyer ethically may accept payments via a Web-based payment-processing service (such as Venmo or PayPal), including funds that are the property of a client or third person, as long as reasonable steps are taken to protect against inadvertent or unwanted disclosure of information regarding the transaction and to safeguard funds of clients and third persons that are entrusted to the lawyer.

Opinion here

The Committee sees no ethical prohibition per se to using these services, as long as the lawyer fulfills certain requirements. Those requirements differ depending on the purpose of the payment—i.e., whether the funds are the property of the lawyer (such as earned fees) or the property of a client or third person (such as advances for costs and fees and escrow deposits). The two principal ethical issues are (1) confidentiality and (2) safeguarding funds of clients and third persons that are entrusted to the lawyer.

For lawyers, accepting payment through a payment-processing service risks disclosure of information pertaining to the representation of a client in violation of Rule 4-1.6(a) of the Rules Regulating The Florida Bar. Rule 4-1.6(a) prohibits a lawyer from revealing information relating to representation of a client absent the client's informed consent. This prohibition is broader than the evidentiary attorney-client privilege invoked in judicial and other proceedings in which the lawyer may be called as a witness or otherwise

Prior to using a payment-processing service, the lawyer must diligently research the service to ensure that the service maintains adequate encryption and other security features as are customary in the industry to protect the lawyer's and the client's financial information and to preserve the confidentiality of any transaction. The lawyer must make reasonable efforts to understand the manner and extent of any publication of transactions conducted on the platform and how to manage applicable settings to preempt and control unwanted disclosures.

Opinion here

← **Tweet**

Christopher Hopkins
@cbhopkins

Pro tip - change your #Venmo account so it is not "public."

1. In app, tap 3 lines in upper right
2. Settings
3. #Privacy
4. Pick Friends or, better, Private

Wait! Your past transactions are still public. Go to Settings/Privacy & "Past Transactions"

Topics

- What is ESI / e-Discovery?
- How Do You Do This?
- What Are the Rules?
- Walk Me Through the Steps
- Recent ESI Cases
- Social Media Discovery
- Alexa & Zoom
- Articles / Handouts

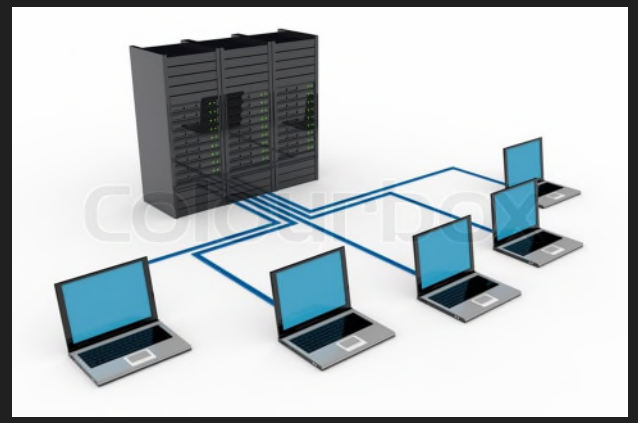
Why Does a Mediator Need To Know ESI & e-Discovery?

- Probably new to you
- COST
- Sanctions
- Need for e-Discovery Mediators
- No case law on point (parties need help)

What is ESI & e-Discovery?

ESI & e-Discovery

McDonald Hopkins



Electronically Stored Information (ESI) [noun]

- Information created, modified, transmitted via software and hardware. "Stuff on a computer"
- *Emails, IM/Texts, Word, Photos, Excel, Video…*
- Hard drive – little "platter" in your PC or laptop
- Phone – solid state drive (SSD)
- Server – "serves" the "client" (your device).
- Cloud – server based somewhere else (vs local)

ESI & e-Discovery

McDonald Hopkins

Metadata *[noun]*

- Data about data / "meta" (self-referential, conscious of self)
- Descriptive, structure, administrative
- Word doc – who created, modified, what changed?
- Image – GPS, device, etc
- Generally used to authenticate, time-stamp, or find people who "touched" the data
- This is why people want "native" format

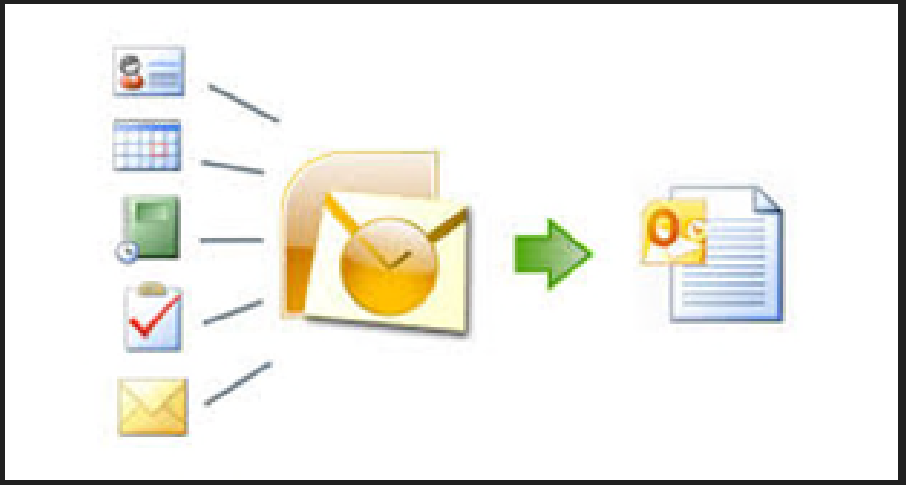
ESI & e-Discovery

McDonald Hopkins

Native format [noun]

- file that is maintained in its original format
- Example: you created a document in WORD, but you e-mailed it as a PDF. Which is the Native format?
- Look for the step of converting to a “foreign” format
- In production, ESI is often converted to PDF or TIFF formats
- Native preserves the original metadata

PST file [noun]



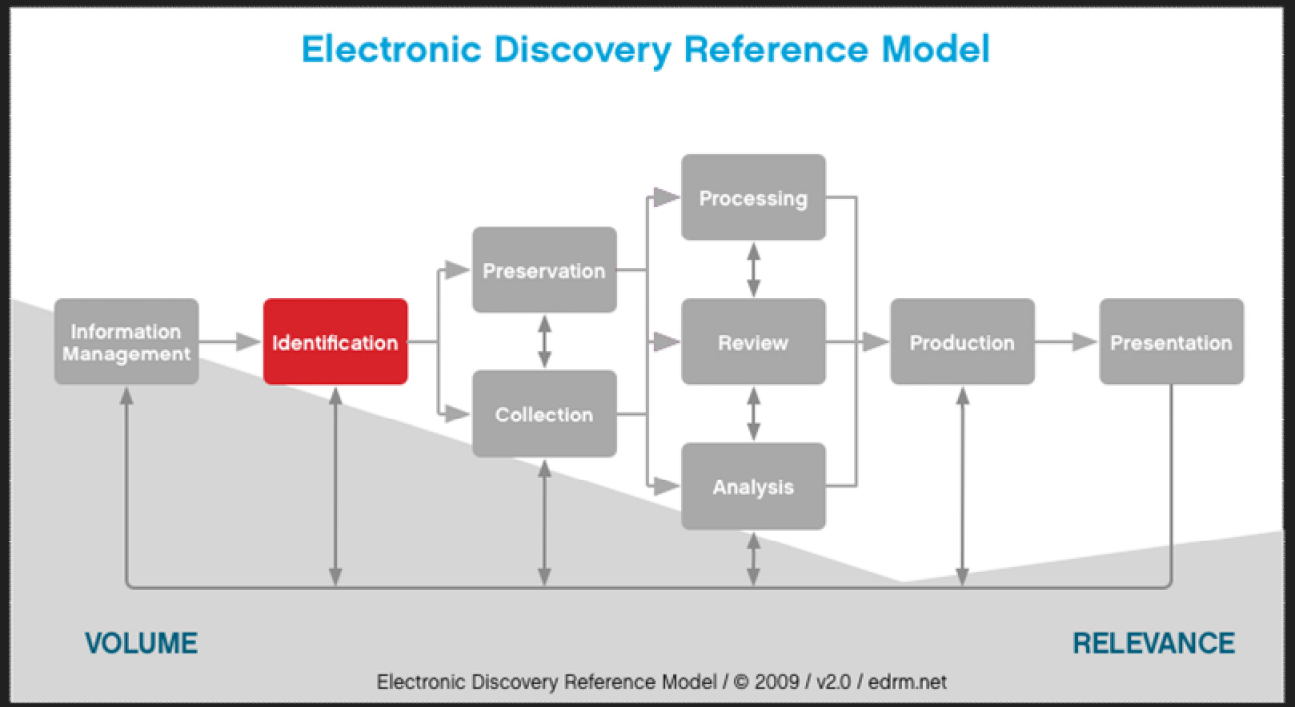
- Personal Storage Table
- This is an example of (most common) ESI
- Microsoft email and calendar files
- Export all emails / calendar events into a file
- Native format. Searchable. Has metadata

ESI & e-Discovery

McDonald Hopkins

E-Discovery [noun]

- Discovery of information in an electronic format (ESI)
- Federal Rules revised in 2006 EDRM
- Identify.
- Preserve.
- Collect.
- Review.
- Produce

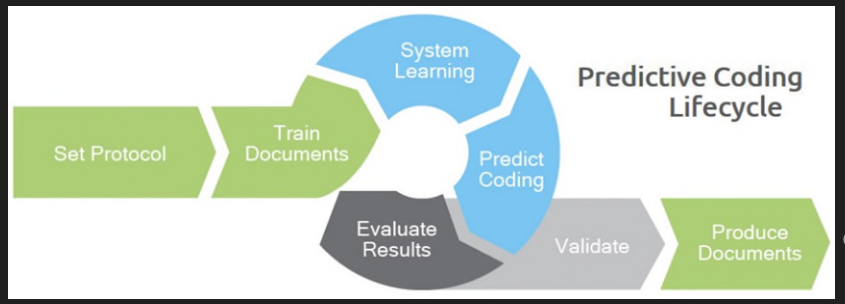


How Do We Find ESI?

ESI & e-Discovery

Predictive Coding

McDonald Hopkins



- Machine-learning technology which enables the computer to “predict” how documents should be classified based upon limited human input
- “training set” – subset of documents used to train the system
- “control set” – sample of documents used to test the responsiveness of the predictive coding
- “yield” – e.g., 200,000 documents out of 1m match criteria, yield is 20%
- Saves money over “word search”

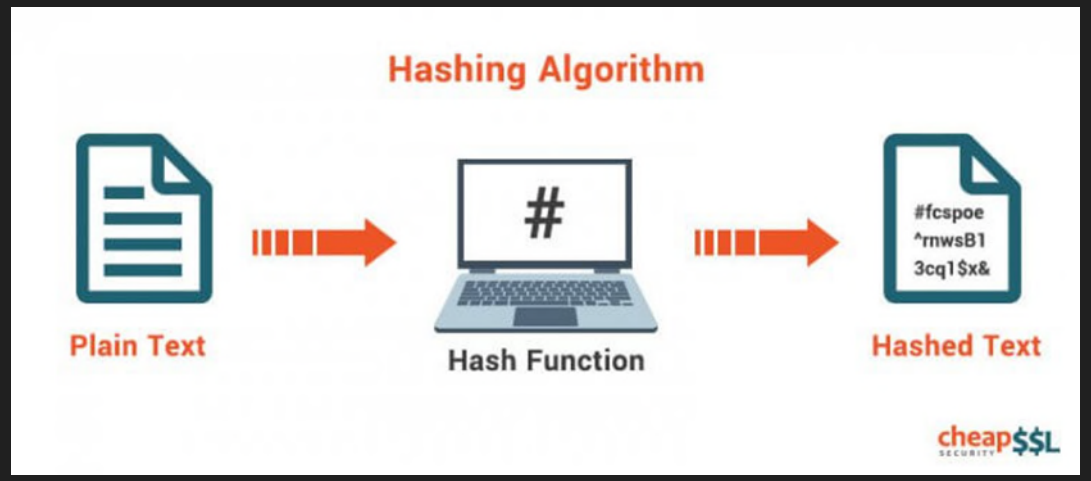
CAR and TAR

- Computer Assisted Review
- Technology Assisted Review – software used to compare and analyze documents (to find differences or similarities).
- *Looking for patterns*
- *Predictive coding is a type of CAR*
- "Discussion threading" – links related documents together, such as emails in a chronological string (helps identify who was involved and when)

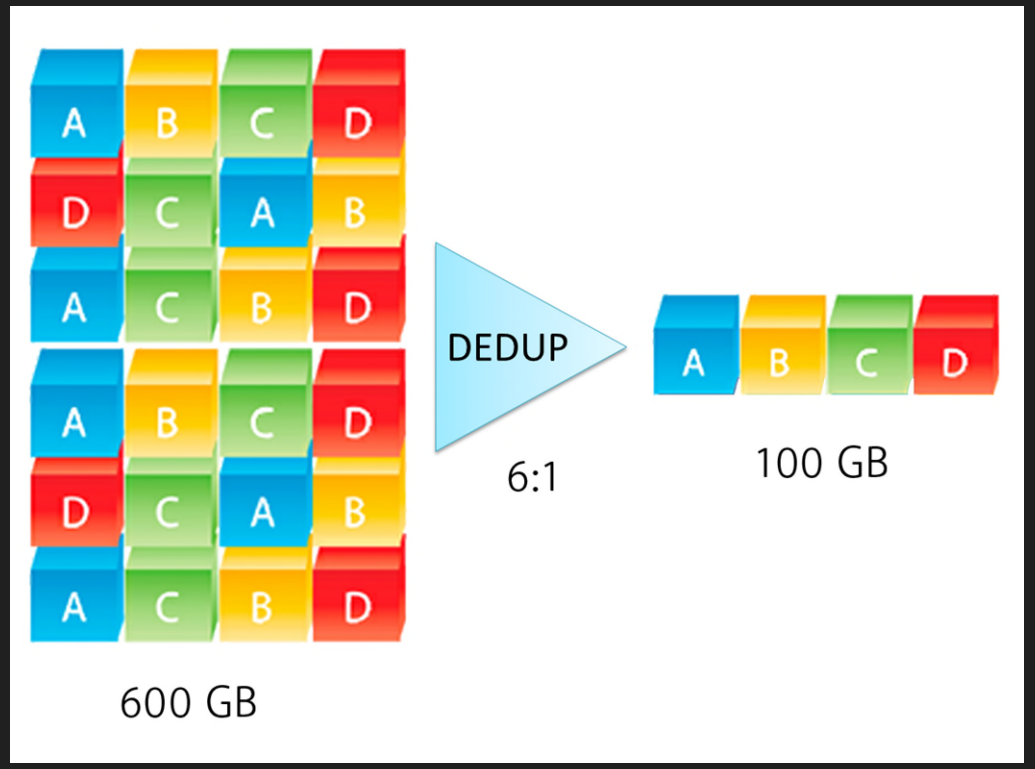
ESI & e-Discovery

Hash

- Algorithm creates a unique value for each document
- Digital fingerprint
- Helps authenticate AND identify duplicates
- Think “hashtag” in social media



McDonald Hopkins



De-Duplicating

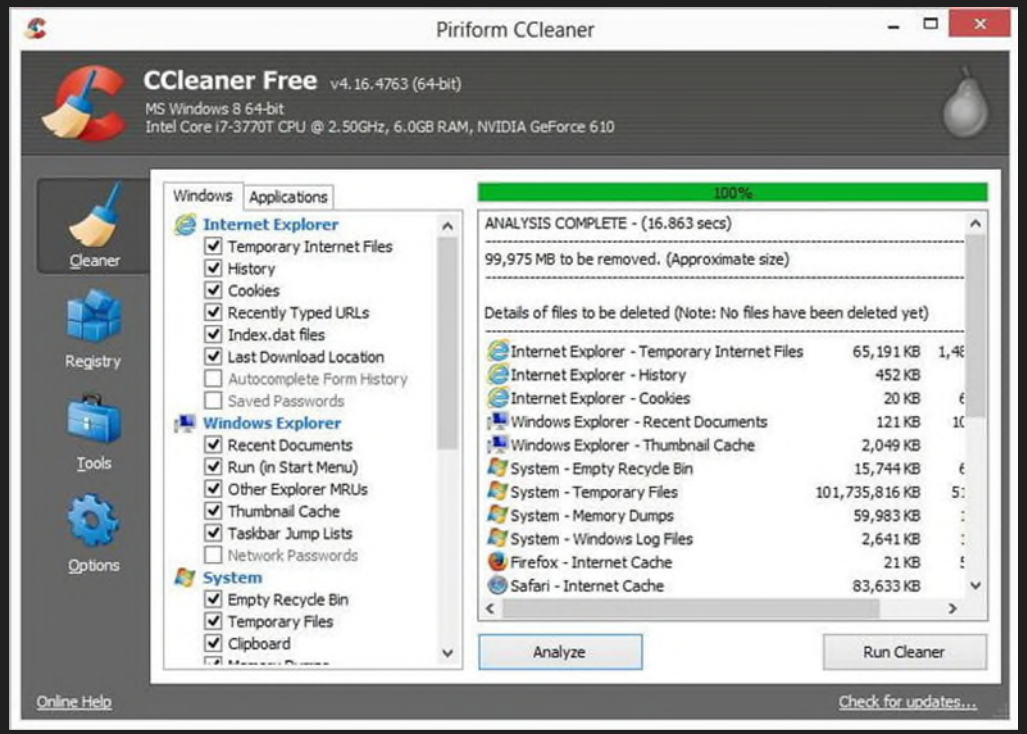
- Aka “de-duping”
- Compare documents to remove duplicates
- Reduces review time
- *You use “hash” values to find/remove duplicates!*

De-NIST-ing

- NIST has the National Software Reference Library – list of known computer applications
- To De-NIST means to identify unimportant computer system files and remove from your document collection
- *Getting rid of junk files*
- *ROT – redundant, obsolete, trivial*

ESI & e-Discovery

McDonald Hopkins



Slack Space

- Un-used portion of a disk/drive
- ~ *"Unallocated space"* – where file is marked for deletion / over-writing but is not "gone" yet
- *Sometimes hear the word "cache"*
- Examples: Criminal case (porn) and to find fraud (deleted documents)

What Are The Rules?

ESI & e-Discovery

Florida E-Discovery Rules

Effective September 1, 2012

McDonald Hopkins

Case Management Rule 1.200
* Court can make advanced ruling on admissibility; facilitate agreement on scope, form, limits
* Federal rule requires "meet & confer" FL only requires meeting in complex cases

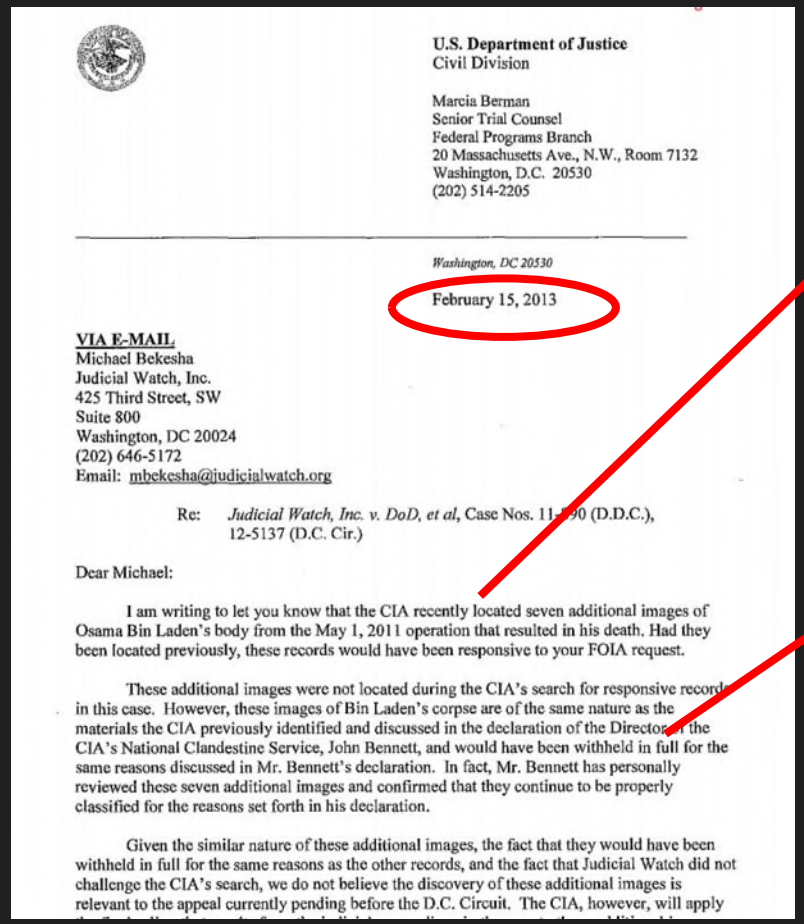
Scope and Limits Rule 1.280
ESI is discoverable but with limits similar to Fed Rule 26
ESI "not reasonably accessible" is not discoverable absent good cause
Costs can be shifted
Proportionality and Reasonableness factors

Request for Production Rule 1.350
Requesting party can specify file format

Subpoenas Rule 1.410
Respondent may object to form or not reasonably accessible
Can be ordered for good cause
Costs can be shifted
Respondent must produce in ordinary or reasonably usable form
FRCP 45 has sanction for subpoenas which are burdensome

Sanctions Rule 1.380
No sanctions, absent exceptional circumstances, for failing to produce EHI as a result of "routine, good-faith operation of an electronic information system."

Even the CIA Makes Mistakes



U.S. Department of Justice
Civil Division

Marcia Berman
Senior Trial Counsel
Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7132
Washington, D.C. 20530
(202) 514-2205

Washington, DC 20530

February 15, 2013

VIA E-MAIL
Michael Bekesha
Judicial Watch, Inc.
425 Third Street, SW
Suite 800
Washington, DC 20024
(202) 646-5172
Email: mbekesha@judicialwatch.org

Re: *Judicial Watch, Inc. v. DoD, et al*, Case Nos. 11-590 (D.D.C.), 12-5137 (D.C. Cir.)

Dear Michael:

I am writing to let you know that the CIA recently located seven additional images of Osama Bin Laden's body from the May 1, 2011 operation that resulted in his death. Had they been located previously, these records would have been responsive to your FOIA request.

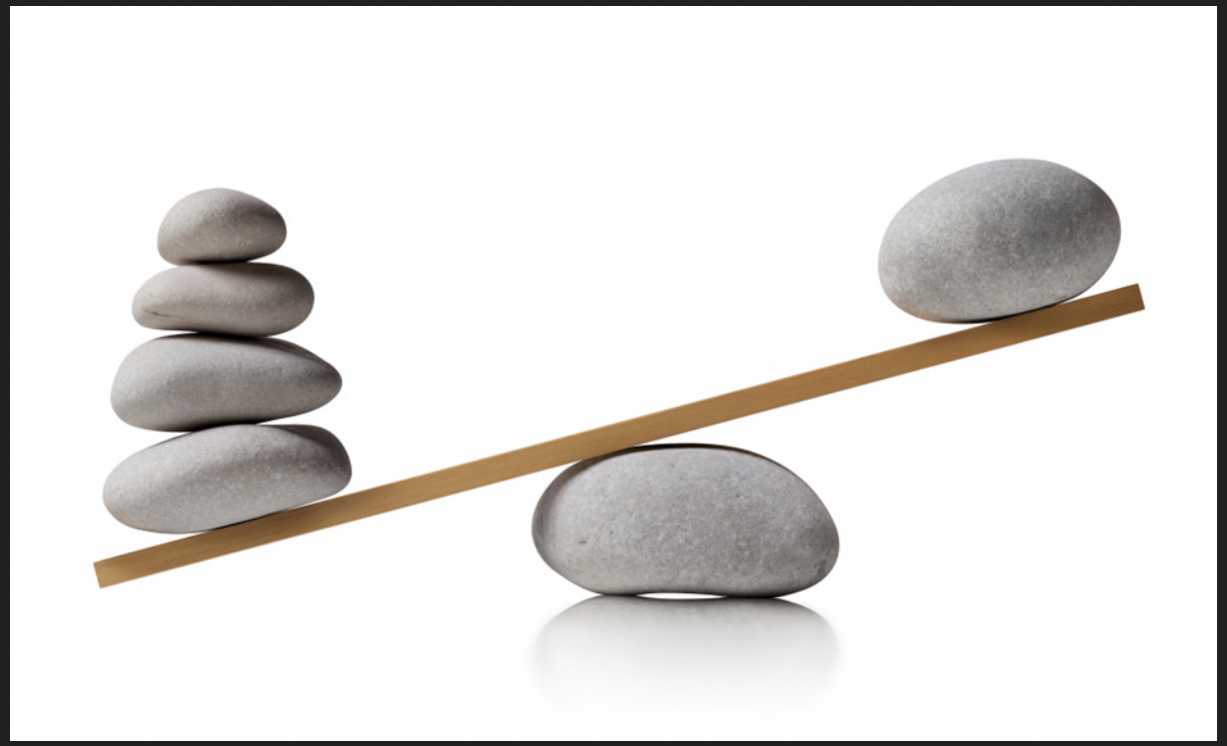
These additional images were not located during the CIA's search for responsive records in this case. However, these images of Bin Laden's corpse are of the same nature as the materials the CIA previously identified and discussed in the declaration of the Director of the CIA's National Clandestine Service, John Bennett, and would have been withheld in full for the same reasons discussed in Mr. Bennett's declaration. In fact, Mr. Bennett has personally reviewed these seven additional images and confirmed that they continue to be properly classified for the reasons set forth in his declaration.

Given the similar nature of these additional images, the fact that they would have been withheld in full for the same reasons as the other records, and the fact that Judicial Watch did not challenge the CIA's search, we do not believe the discovery of these additional images is relevant to the appeal currently pending before the D.C. Circuit. The CIA, however, will apply

…let you know that the CIA recently located 7 additional images of OBL's body… Had they been located previously, these records would have been responsive to your FOIA request…

…we do not believe the discovery of these additional images is relevant to the appeal pending currently before the D.C. Circuit.

McDonald Hopkins

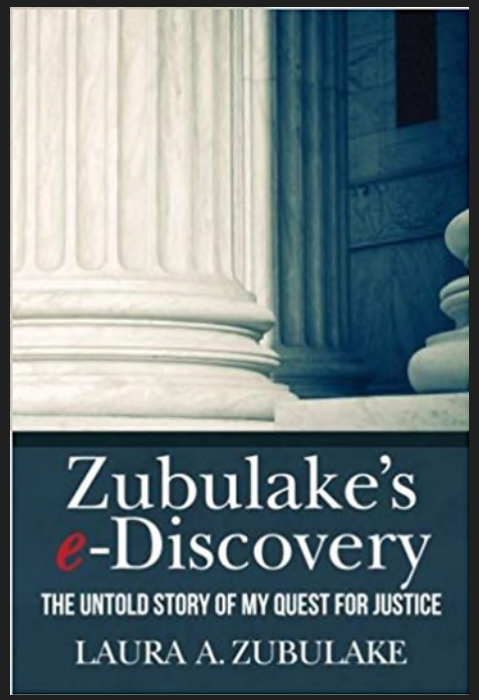


Proportionality

- Rule 1.280 & FRCP 26
- Reasonably accessible?
- Cost shifting
- *A mediator or special master may help focus need & cost issues*

ESI & e-Discovery

McDonald Hopkins



Series of opinions in
Zublake v. UBS Warburg

Prior to 2006 federal amendments
Issued by Judge Scheindlin (now retired)

7-factor test for cost shifting based upon accessibility (harder it is, more likely to get shifted to requesting party)

Case is famous because:

- Scope of duty to preserve ESI
- Lawyer's duty to monitor client's litigation hold
- Knowing cost and effectiveness of recovery in advance
- Shifting costs to requesting party
- Spoliation

ESI & e-Discovery

McDonald Hopkins

Technology Corner

Will Judge Sasser's Standing ESI Order Apply to Your Case?

by Christopher B. Hopkins

Do you know what a .pst file is? Have you created a client data map? What is the difference between system and substantive metadata? Lawyers can no longer ignore or avoid e-discovery – the preservation and production of electronically stored information (ESI) – since the practice was embedded in the Florida Rules of Civil Procedure in 2012. Starting July 1, 2016, Judge Meenu Sasser of the Fifteenth Judicial Circuit has issued a Standing Order on Electronically Stored Information Discovery to both coax and compel lawyers into discussing and addressing ESI discovery. This article will re-introduce you to Florida's e-discovery rules, provide an overview of Judge Sasser's Standing Order, and identify resources for handling e-discovery issues in your cases.

In 2012, the Florida Rules of Civil Procedure were amended to include e-discovery. The amendments are similar but less demanding than their federal counterparts; Rule 1.200 states that a case management order "may" require lawyers to "consider" ESI admissibility and "discuss" the "possibility" of ESI agreements. Rule 1.280 more forcefully establishes ESI as a part of discovery and articulates the boundaries of what is "reasonably accessible." Rule 1.350 explains the form of ESI production and Rule 1.380 defines sanctions for failure to preserve ESI.

the client and obtain ESI info
and confer, counsel needs to
various ESI issues. It is advis
and a summary of the e-disc
understand the necessary ste
practical, counsel should issu
with Rule 1.380.

In preparation for the me
obtain information such as: i
of the client's system and em
relevant information or infor
lead to discovery of admissib
nature of ESI policies; and id
Typically, it is not difficult t
however it can be surprisingl
accurate "data map" of where
phones, backups, cloud, IM,
most companies use suites li
database, time-keeping, and
for landmarks such as when
major software change or ha
data harder to access. Again,
and not production.

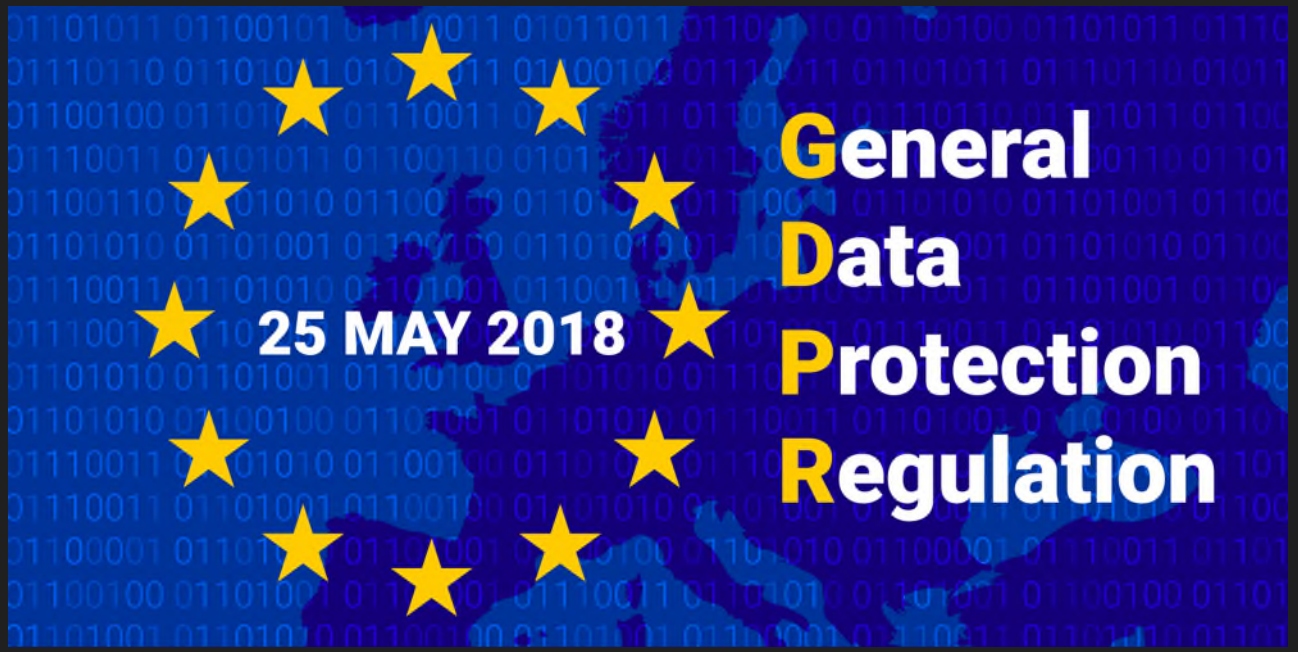
The "meet and confer" s
since it requires counsel to "

Standing ESI Order

- Some judges are creating standard orders setting out how to handle e-Discovery
- ASK your parties if there is a judge- or jurisdiction-specific ESI order… *just as you would ask if they are set for trial.*
- *Or if you can give them one.*

ESI & e-Discovery

McDonald Hopkins



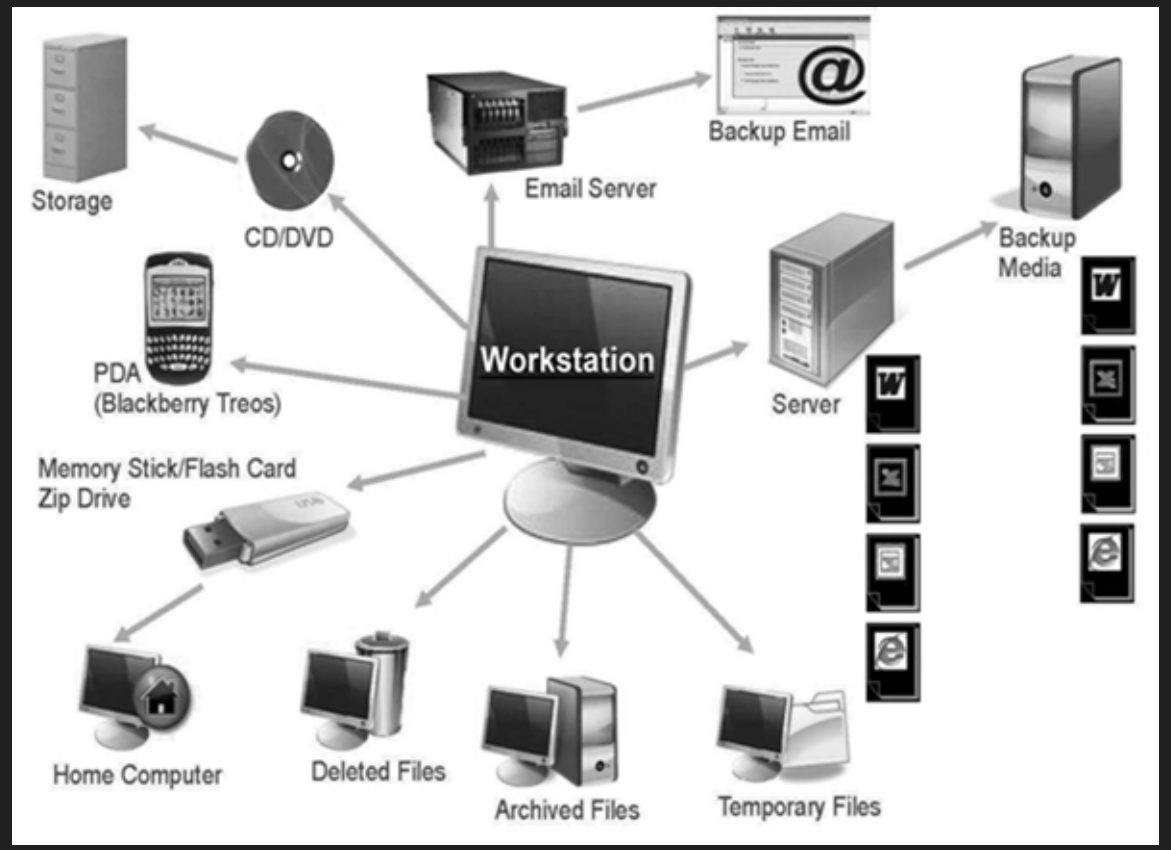
GDPR

- NOT a U.S. law but international corporations are following.
- Likely to become a standard
- Helps data protection and privacy since parties are getting rid of data
- Requires a “data protection officer”
- GDPR compliance likely means a party has better organized data

Walk Me Through the Steps

ESI & e-Discovery

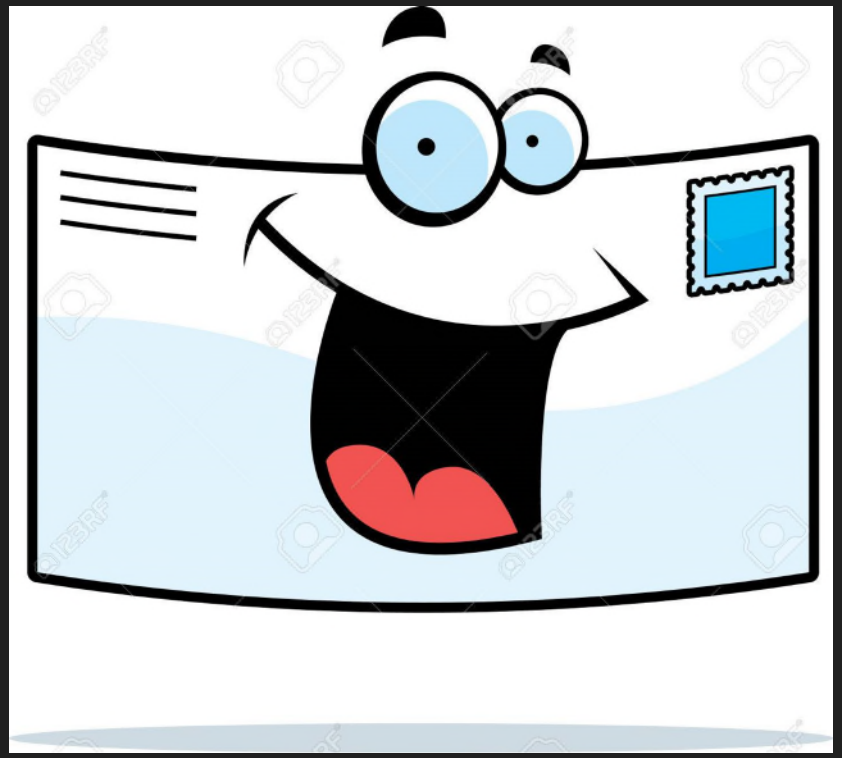
McDonald Hopkins



Data Map

- BEFORE litigation or e-discovery, companies should have a chart where they store data
- This is an IT and LEGAL department issue
- *TIP: ask your litigants if they have a data map.*

McDonald Hopkins



Preservation Demand Letter

- Notice to (potential) opposing party to preserve necessary evidence and information.
- Typically tells the other side to stop any sort of auto-delete per the company's deletion policy (e.g., think GDPR compliance).
- Could be a setup for spoliation claim.

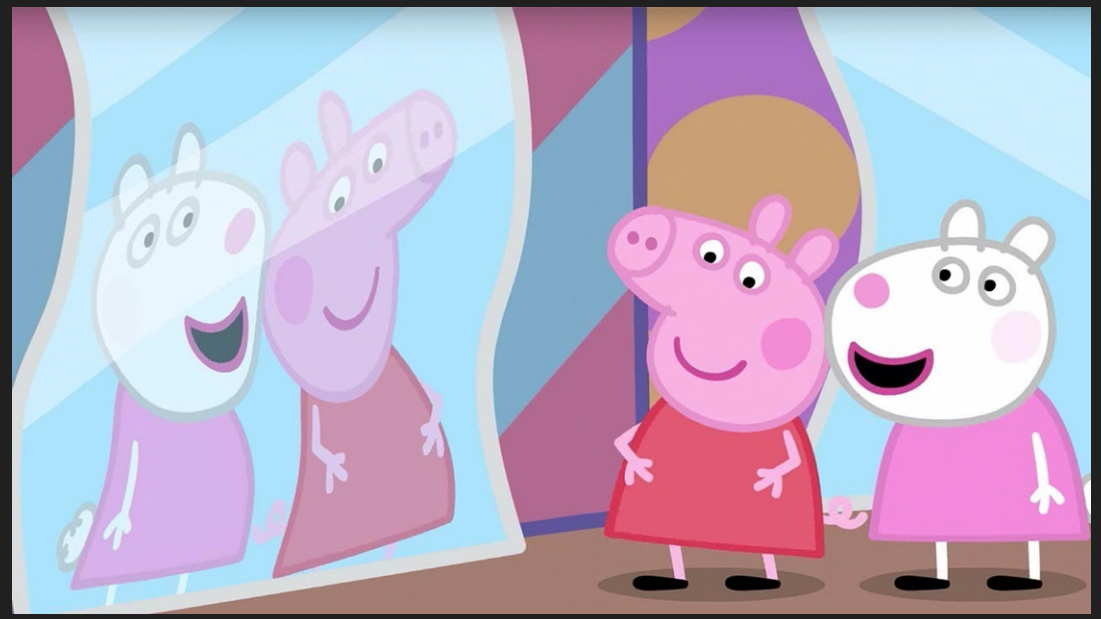
McDonald Hopkins

Litigation (or Legal) Hold

- Notification sent by a company's legal team (typically) to employees and other departments with instructions not to delete or destroy documents
- BEFORE there is a case
- Can be in response to a Preservation Demand or on its own
- This is an INTERNAL process

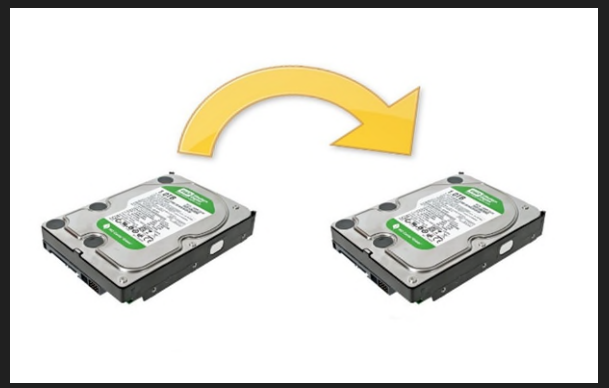
ESI & e-Discovery

McDonald Hopkins



"Image" a drive vs. "image" a file

- Image (a drive): make an identical copy of a drive, including its slack and unallocated space.
- Image (a file): make a picture copy of a file, such as PDF or TIFF.
- *Think "mirror image"*



Example: Warrant in Las Vegas Shooter Case

Litigants can / should learn from law enforcement how to phrase their e-discovery requests

ATTACHMENT "A1"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Accounts") from their inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

Warrant in Las Vegas Shooter Case

ESI

which the Government sought from Microsoft (email account provider)

a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;

d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.

e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

Warrant in Las Vegas Shooter Case

Metadata which the Government sought from Microsoft (email account provider)

a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;

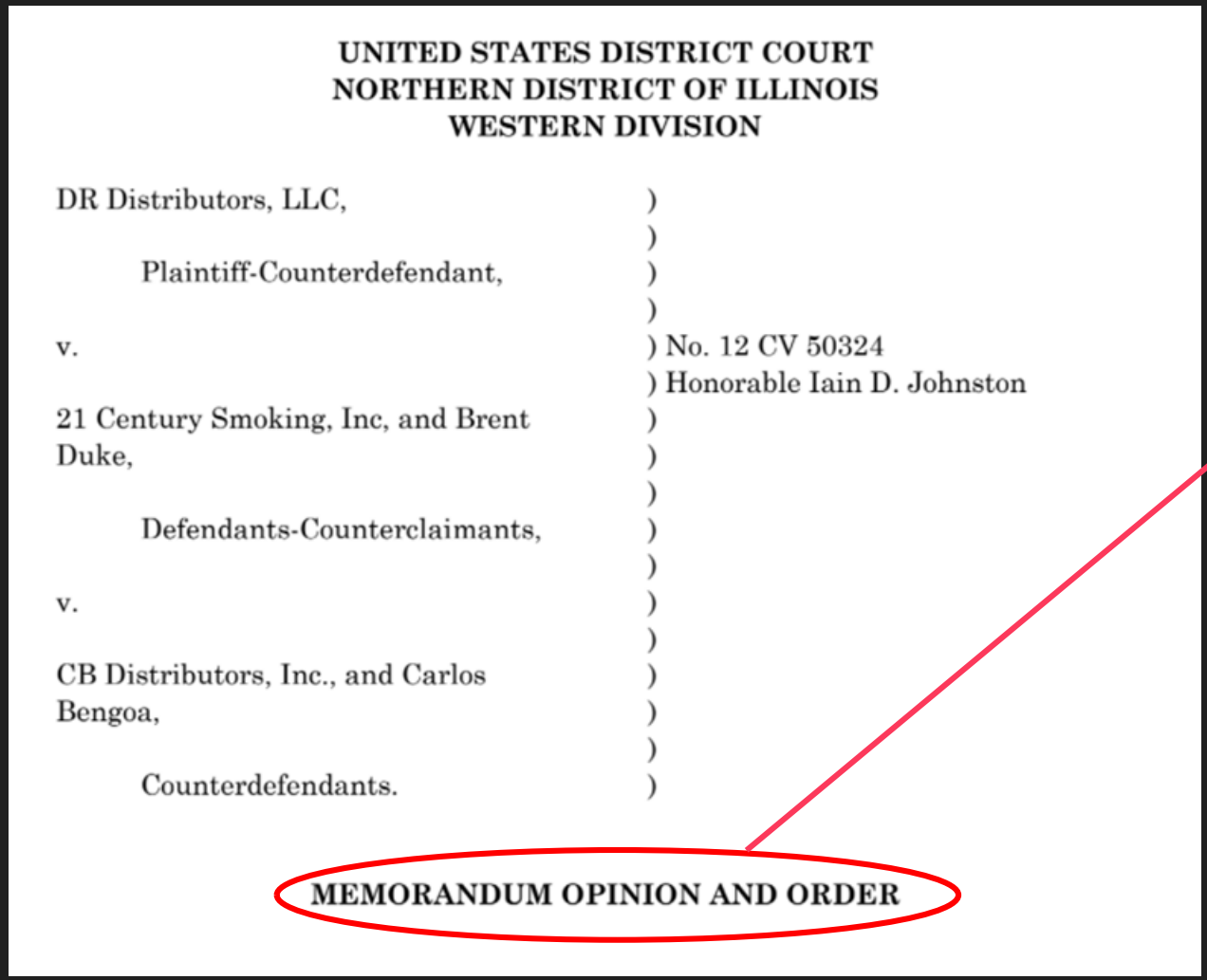
d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.

e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

Recent ESI Cases

Recent ESI Cases

McDonald Hopkins



UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
WESTERN DIVISION

DR Distributors, LLC,

Plaintiff-Counterdefendant,

v.

21 Century Smoking, Inc, and Brent Duke,

Defendants-Counterclaimants,

v.

CB Distributors, Inc., and Carlos Bengoa,

Counterdefendants.

No. 12 CV 50324
Honorable Iain D. Johnston

MEMORANDUM OPINION AND ORDER

256 pages?!!!

(a 2021 book on ESI pitfalls)

Recent ESI Cases

McDonald Hopkins

"Snakebit" – That's how former defense counsel described this case. But "snakebit" connotes the unfortunate circumstances that befall unsuspecting victims. That didn't happen here. Instead, through a series of missteps, misdeeds, and misrepresentations, Defendants and former defense counsel find themselves looking down the barrel of a sanctions motion Howitzer.

Recent ESI Cases

McDonald Hopkins

- Court asked if there were litigation holds
- No one told the court that none had been issued
- The parties had not discussed ESI search terms
- Perfection is not the standard
- Don't need to be ESI experts
- All you had to do was Google search to find out the difference between Yahoo Chats and Yahoo Mail and how to save
- Client was not clear or "at worst… deceived his attorneys into believing all the relevant electronic records were stored on his hard drive."

Recent ESI Cases

McDonald Hopkins

"…the Court is fully aware that Plaintiff's request for attorney's fees and costs will likely exceed seven figures…"

Recent ESI Cases

McDonald Hopkins

JOHN DOE, Plaintiff,

v.

PURDUE UNIVERSITY, et al., Defendants.

Cause No. 2:17-CV-33-JPK.

United States District Court, N.D. Indiana, Hammond Division.

July 2, 2021.

OPINION AND ORDER

JOSHUA P. KOLAR, District Judge.

This matter is before the Court on a Request for Issuance of Order to Show Cause Regarding Plaintiff's Non-Compliance with Order and Spoliation of Evidence [DE 133], filed by Defendants Purdue University, Purdue University Board of Trustees, Michell Elias Daniels, Jr., Alysa Christmas Rollock, and Katherine Sermersheim. The Court held an evidentiary hearing on this issue on February 22, 2021, and the parties filed supplemental briefing on April 27, 2021. For the following reasons, the motion is granted with relief different than requested.

Recent ESI Cases

McDonald Hopkins

INTERROGATORY

Identify all social media websites or applications that you used, participated on, posted photos, opinions, or statuses, or otherwise had an account with/on at any point during or after August 2015 and for each state your username, account name, or any other identifier for your account."

Recent ESI Cases

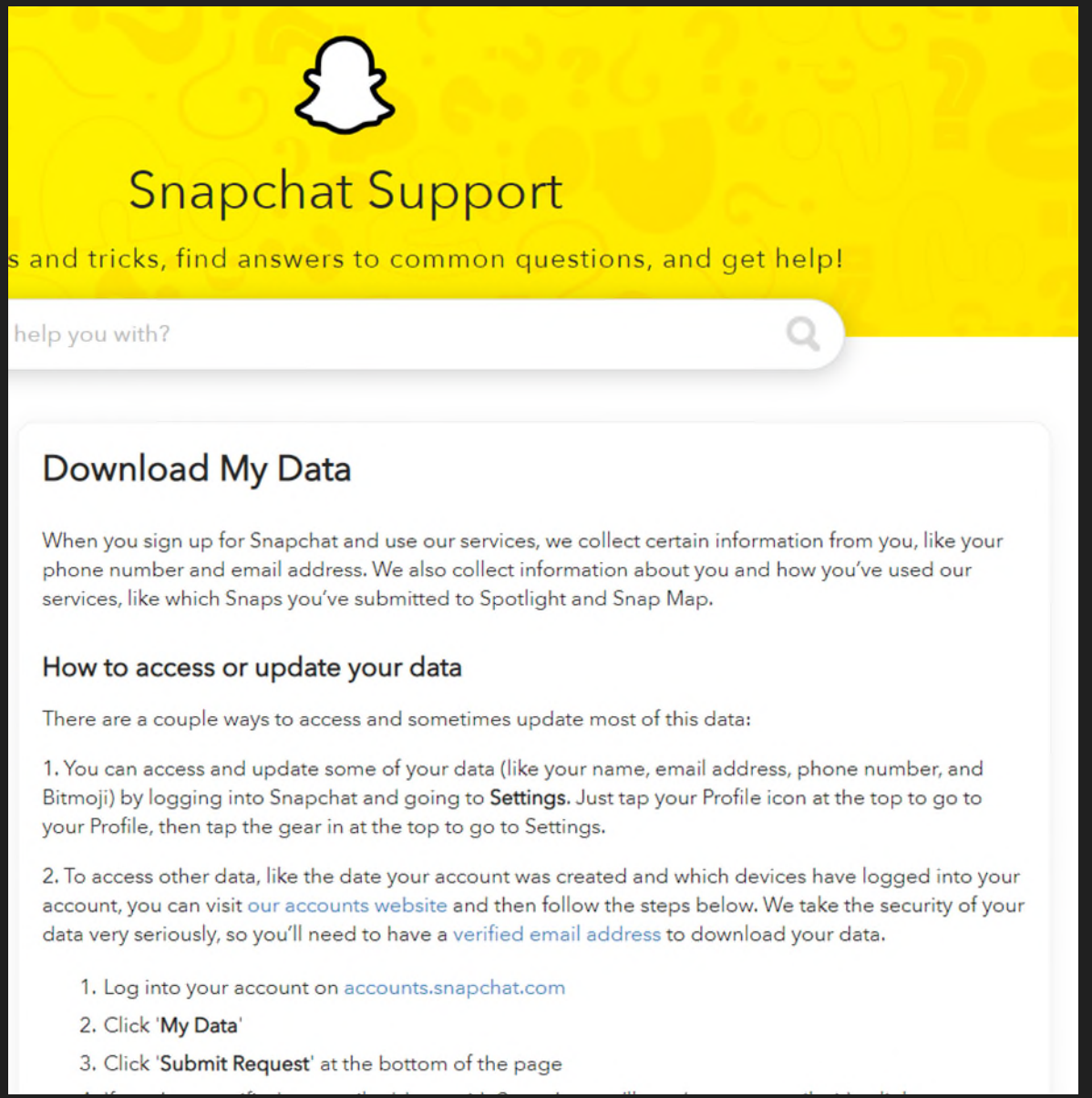
McDonald Hopkins

RFP: Produce all of Plaintiff's social media postings from August 2015 to present.

This data is the property of the Plaintiff and may be obtained and downloaded in its entirety as set forth in the following link: https://support.snapchat.com/en-US/a/download-my-data

Recent ESI Cases

McDonald Hopkins



Snapchat Support

s and tricks, find answers to common questions, and get help!

help you with?

Download My Data

When you sign up for Snapchat and use our services, we collect certain information from you, like your phone number and email address. We also collect information about you and how you've used our services, like which Snaps you've submitted to Spotlight and Snap Map.

How to access or update your data

There are a couple ways to access and sometimes update most of this data:

1. You can access and update some of your data (like your name, email address, phone number, and Bitmoji) by logging into Snapchat and going to **Settings**. Just tap your Profile icon at the top to go to your Profile, then tap the gear in at the top to go to Settings.

2. To access other data, like the date your account was created and which devices have logged into your account, you can visit our accounts website and then follow the steps below. We take the security of your data very seriously, so you'll need to have a verified email address to download your data.

   1. Log into your account on accounts.snapchat.com
   2. Click '**My Data**'
   3. Click '**Submit Request**' at the bottom of the page

Recent ESI Cases

McDonald Hopkins

- Plaintiff and counsel filed declarations that Snapchat "does not retain user identity past 30 days."
- Plaintiff produced a Snapchat download contained broken links to 86 photos.
- A new production had 11 less links.
- Plaintiff had deleted them from his phone "to save space"

Recent ESI Cases

McDonald Hopkins

- "The duty to preserve evidence certainly arises upon a formal discovery request" (likely it's late)
- Often there's a (federal) court order requiring parties to preserve ESI
- "The argument advanced by Plaintiff's counsel – that Plaintiff did not intentionally destroy anything – is meaningless in this context."

Recent ESI Cases

McDonald Hopkins

CIVIL NO. 4:19-CV-140-SDJ
UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS SHERMAN DIVISION

Edwards v. Junior State of Am. Found.

Decided Apr 23, 2021

CIVIL NO. 4:19-CV-140-SDJ

04-23-2021

DANIEL EDWARDS, JR., ET AL. v. JUNIOR STATE OF AMERICA FOUNDATION, ET AL.

Harper was JSA's student Governor of Texas, and Edwards, Jr. sought a position in Harper's cabinet.

2 *2

On August 10, 2015, Daniel Edwards, Sr.—Daniel Edwards, Jr.'s father—filed a complaint with JSA,

Recent ESI Cases

McDonald Hopkins

- Student #1 allegedly sends racist and homophobic Facebook messages to student #2
- At scheduling conference, discuss need to preserve ESI
- Discovery for Facebook Messenger communications
- Student #2 had deleted his FB Account.
- FB messages can easily be faked.
- No metadata to prove authenticity

Recent ESI Cases

McDonald Hopkins

"To preserve the ESI in question, [student #2] needed only to *not permanently delete* his Facebook account long enough to download the files in question, a step which only takes a brief series of clicks and a matter of seconds…"

Recent ESI Cases

McDonald Hopkins

Civil No.: 20-cv-80148-SINGHAL/MATTHEWMAN
UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA

Measured Wealth Private Client Grp. v. Foster

Decided Mar 31, 2021

Civil No.: 20-cv-80148-SINGHAL/MATTHEWMAN

03-31-2021

MEASURED WEALTH PRIVATE CLIENT GROUP, LLC, a New Hampshire limited liability company, Plaintiff, v. LEE ANNE FOSTER, an individual, et al., Defendants.

WILLIAM MATTHEWMAN United States Magistrate Judge

[2] The sealed exhibits to the reply are at DE 163.

The discovery issue currently pending before the Court is whether Plaintiff should be permitted to conduct a forensic examination of Defendant Lee Anne Foster's mobile phone to recover certain text messages and iMessages from the period of January 1, 2019 through December 31, 2019. In response, Defendant asserts that the temporal scope is too broad and would result in the production of irrelevant text messages and

Recent ESI Cases

McDonald Hopkins

- Dispute over iMessages on Defendant's iPhone
- Plaintiff had sent proper discovery requests
- "Court wants to put an end to this discovery dispute and finds that a forensic examination, with necessary safeguards to protect Defendant's privacy, is the best way to accomplish the task."
- "…the Court is concerned that Defendant's search of her phone was inadequate."

Protocol to Search Device

- Independent expert appointed by the Court shall mirror the phone. Parties can agree or submit names of experts.
- Expert is an officer of the Court.
- Parties agree on search terms or submit a list and Court decides.
- Expert searches the mirrored image for the search terms.
- Defendant reviews and gets a chance to object.
- Plaintiff pays.
- If data recovered is something Defendant could have produced, Court will consider charging cost.
- Expert shall sign affidavit of steps taken.

Social Media Discovery

Social Media Discovery

McDonald Hopkins

Ten Steps to Obtain Facebook Discovery In Florida

By Christopher B. Hopkins

The number of appellate decisions setting out standards for litigants pursuing discovery of information posted on social media websites is small, but growing. In this article Christopher Hopkins identifies trends in the decisional law and suggests ten steps that will improve the chances of obtaining social media discovery. The article focuses on Facebook, but the principles described here can be applied to other social and professional networking sites.

In the past year, three Florida appellate courts have articulated standards in civil cases for the discovery of content from a party's Facebook account. Before 2014, Florida's scant precedent for social media discovery was composed of two federal and two state trial court orders. While this budding authority of three opinions and four orders is not fully harmonized, defense practitioners will detect trends and strategies for obtaining Facebook content (*e.g.*, posts, comments, still images, video, or other information) and, potentially, full access to a plaintiff's Facebook account.

Rather than serving a standard set of "social media discovery" requests, the lesson from these Florida cases is that defense counsel should take discrete steps — early in the case, followed by narrow social media discovery in stages— to maximize production of the plaintiff's Facebook content. This article provides an overview of the recent social media discovery rulings in Florida; explains the grounds to overcome frequent plaintiff objections; and describes ten steps to obtain court-approved access to the plaintiff's Facebook content.

A primer on Facebook and other forms of social media is likely not necessary for most Florida lawyers.[1] This article will focus exclusively on Facebook because of that site's popularity, but the principles and steps articulated here likely will apply to other social media. We begin with a chronological discussion of the four trial court orders from 2011 through 2013 and the more recent 2014 through 2015 appellate opinions.

"Facebook Discovery" Trial Court Orders 2011–2013

There are four reported Florida trial court orders regarding Facebook discovery, decided by the Broward and Palm Beach County circuit courts and the Middle District of Florida. The two South Florida trial court orders — *Beswick v. Northwest Medical Center, Inc.* and *Levine v. Culligan* — are the most significant.

Beswick v. Northwest Medical Center, Inc.[2]

The earliest reported authority in Florida articulating standards for the discovery of a plaintiff's Facebook account is the November 2011 Broward County circuit court order in *Beswick v. Northwest Medical Center, Inc. Beswick* is also noteworthy because it was relied upon by two of the six subsequent Florida cases.[3]

The *Beswick* defendant sent discovery requests asking one of the plaintiffs to identify her social media accounts and to divulge a copy of all shared content for the preceding five years.[4] The *Beswick* plaintiff objected on the grounds that these requests were overbroad, burdensome, not reasonably related to the discovery of admissible evidence, and violative of privacy rights.[5] This mantra of objections, as illustrated below, appears to be the prevailing grounds that plaintiffs use to avoid production of Facebook content.

ABOUT THE AUTHOR...

CHRISTOPHER B. HOPKINS is a member of McDonald Hopkins LLC (West Palm Beach). He received the *Trial Advocate Quarterly* Award in 2012 and has been on the TAQ editorial board since 2004. His litigation and appellate practice frequently focuses on emerging technologies. His email is chopkins@mcdonaldhopkins.com.

Social Media Discovery

McDonald Hopkins

148 So.3d 163
District Court of Appeal of Florida,
First District.

Tammy Lee ANTICO, Personal Representative of the Estate of Tabitha Frances Guyton **Antico**, Deceased, Petitioner,
v.
SINDT TRUCKING, INC., and James Paul Williams, Respondents.

No. 1D14–277. | Oct. 13, 2014.

Synopsis
Background: Estate of driver, who was killed in vehicular collision with **truck**, brought wrongful death action against **trucking** company, which operated **truck**. Company moved for an order from the trial court permitting an expert to inspect data from driver's cellphone on day of the accident. The trial court granted motion. Driver's estate filed petition for writ of certiorari.

[Holding:] The District Court of Appeal, Osterhaus, J., held that trial court did not err by allowing company's expert to retrieve data from driver's cellphone under limited and controlled conditions.

Est of Antico v. Sindt Trucking, Inc.
148 So.3d 163 (Fla. 1st DCA 2014)

- Defendant sought phone and FB content
- NOT IN OPINION = FB implicated because relatives later posted, "don't text and drive."
- Arguably not a "social media" case but same analysis. See also *Restrepo v. Carrera*, 3d DCA (April 13, 2016).

Social Media Discovery

McDonald Hopkins

DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FOURTH DISTRICT

MARIA F. LEON NUCCI and **HENRY LEON,** her husband,
Petitioners,

v.

TARGET CORPORATION, AMERICAN CLEANING CONTRACTING, INC., and **FIRST CHOICE BUILDING MAINTENANCE, INC.,**
Respondents.

No. 4D14-138

[January 7, 2015]

Petition for writ of certiorari to the Circuit Court for the Seventeenth Judicial Circuit, Broward County; John J. Murphy, III, Judge; L.T. Case No. 10-45572 (21).

John H. Pelzer of Greenspoon Marder, P.A., Fort Lauderdale, and Victor Kline of Greenspoon Marder, P.A., Orlando, for petitioners.

Nicolette N. John and Thomas W. Paradise of Vernis & Bowling of Broward, P.A., Hollywood, for respondent, Target Corporation.

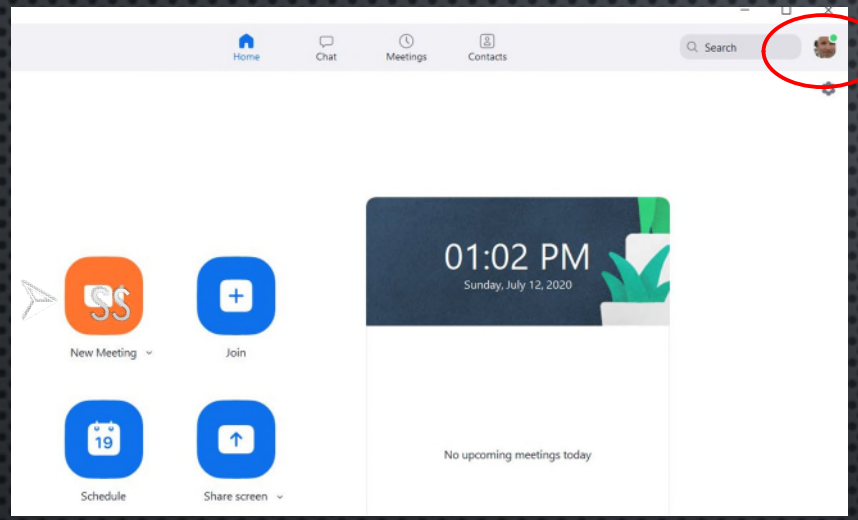
GROSS, J.

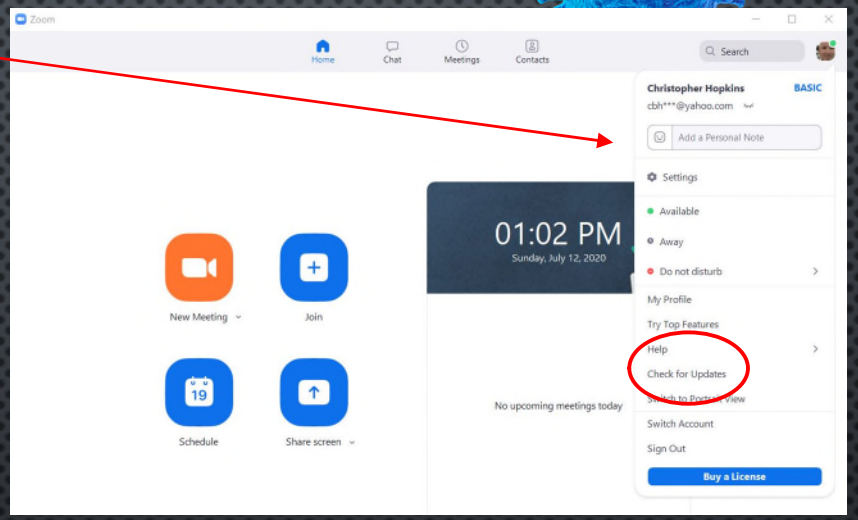
Nucci v. Target Corp.
162 So.3d 146 (Fla. 4th DCA 2015)

- Photos only
- "there is no better portrayal of what an individual's life was like than through those photographs which the individual has chosen to share through social media" (really?)
- "...all content on a Facebook page does not necessarily have the inherent value of a user's photo collection" (Hogwood v HCA Holdings)

Brief Discussion of Zoom & Alexa

USE CURRENT VERSION OF ZOOM





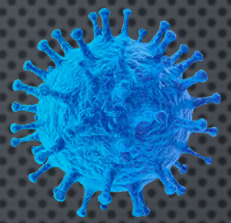
[Zoom's Update Info Page]

SECURELY HOST A MEETING ON ZOOM

- Require a Passcode (on invite; but people can circulate)
- Waiting Rooms (best prevention; difficult w lots of attendees)
- Lock Meetings On Start (Security / Lock Meeting)
- Limit Screensharing:

  (Share Screen / One Participant at a time &/or Only Host)
- Kick Out! (Participants / "More" next to person / Remove)

SECURELY JOIN A MEETING ON ZOOM

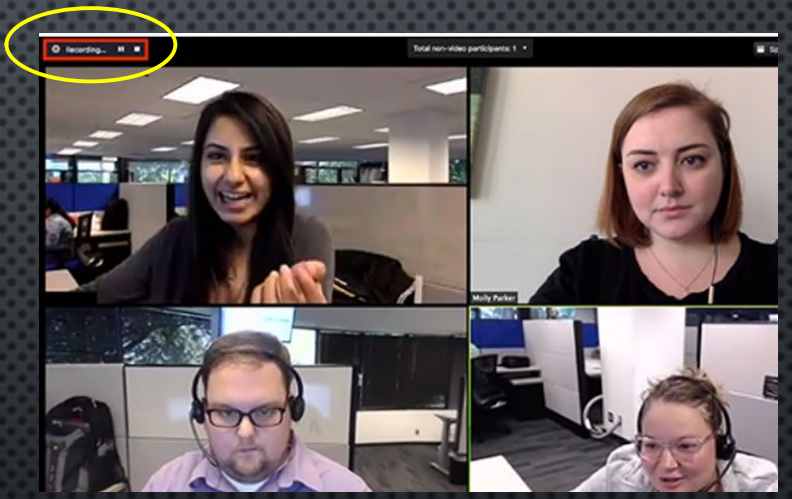


- Auto-Mute Your Audio as you Enter Meeting

  (Settings/Video/Meetings/Turn off my video when joining)
- Auto-Mute Your Video as you Enter Meeting

  (Settings/Audio/My my microphone when joining)
- Use a Virtual Background
- Share Screen… carefully

  (turn off notifications; close tabs; messy desktop)
- *Are You Being Recorded?*

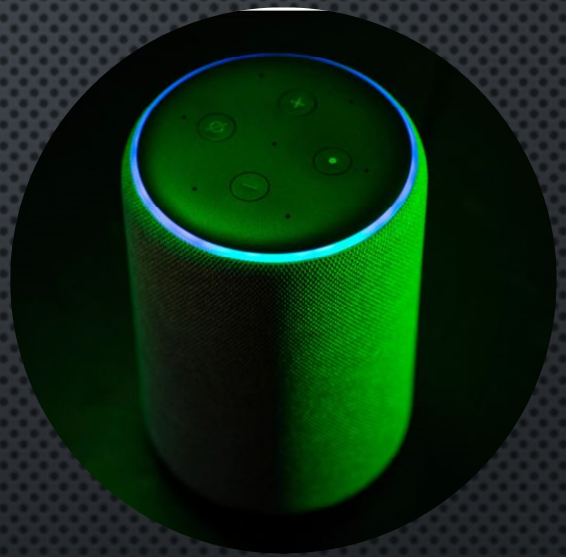



Christopher Hopkins
@cbhopkins
Be aware: people can use #Snap filters or other 3rd party apps on Zoom. But they can also use those apps to *record* your Zoom call. So... even when the red light on the #Zoom app is off, someone can still record your Zoom conference. #privacy #zoomraids #zombie #privacylaw

OF ALL YOUR DEVICES… *ALEXA* IS YOUR CONCERN??

- Set Up Delete By Voice
- What Did She Hear? ("Alexa , tell me what you heard?" "Alexa, why did you do that?")
- Delete Old Recordings (3 or 1 months)
- Unplug or Cover it
- Where's your phone, PC mic, tablet, etc?
- *Sell it? First De-Register & Factory Reset*

Love Zoom but fear Alexa? Up until March 27, 2020, Zoom was sending your data to Facebook!



CNET article & image credit

Christopher's Article on Alexa Privacy

Some Handouts

TECHNOLOGY CORNER

CHRISTOPHER B. HOPKINS

Privacy Settings for Zoom Video and Alexa

In March 2020, as professionals worked from home due to COVID-19, Zoom video conferences surged in popularity while, conversely, lawyers cast weary glances at the Alexa device in their home office, wondering if it was recording confidential communications.

As of this writing, rumors abound on social media about the security of both platforms. With little hard evidence, a BigLaw firm publicly broadcast its ban on these devices. While society struggles with its relationship with ubiquitous communication devices, let us at least properly configure our Zoom and Alexa privacy settings.

Zoom Video: Recommended Settings

As a brief primer, Zoom throws a few numbers at you which can be confusing. A Personal Meeting ID (PMI) is a virtual room assigned to you alone; this is visible on the URL, called a Personal Link, when you invite someone to your personal meeting room. Your Meeting ID is a temporary number for a scheduled meeting. The Meeting ID typically expires after your meeting unless you create a recurring meeting. These links and IDs may be confusing but the important point is that, without proper precautions, they can be hacked, re-used, or simply guessed by third parties.

Is This Being Recorded? - Zoom reports that all participants will see a red notification (upper left on desktop and upper right on iOS) if the meeting is being recorded.

Only the Host Has Certain Abilities - On the website, go to Settings and turn OFF "Join Before Host," "Use Personal Meeting ID," "Annotation," "Remote Control," and "Allow Removed Participants to Rejoin." Meanwhile, turn ON "Allow host to put attendees on hold" and "host only" under screen sharing.

Hypervigilance Against Zoom-Bombing- To really lockdown meetings, on the website, turn off "Join Before Host" and "File Transfer" but turn on "Require Password for... Phone" and, towards the bottom, turn on "Waiting Room." You will need to Google how to use Waiting Rooms.

The following steps will assist in protecting your privacy during a Zoom meeting:

Spacebar To Mute - press and hold spacebar to temporarily mute yourself.

Set a Virtual Background - The benefit of a virtual background is that participants cannot see the room behind you, whether that includes privileged information on a wall calendar or... a snoring pug. Select a high definition shot of the Enterprise, the

Look Your Best - While not strictly a privacy issue, on the desktop app, tap the cog wheel, then video, then Touch Up My Appearance. On iOS, select "more," then Meeting Settings, and turn on Touch Up My Appearance.

Alexa: Recommended Settings

According to Amazon, "you'll always know when Alexa is recording... because a blue light indicator will appear or an audio tone will sound..." What is less clear is what third parties are doing with your data or if voice apps have the power to control the microphone.

What Has Alexa Heard? - In the Alexa app, tap the three lines in the upper left corner and then go to Settings / Alexa Privacy / Review Voice History. Scroll through (and delete) the recent commands she recorded.

Set Up Delete By Voice Command - Following those same steps, toggle on "Enable deletion by voice." Then later you can instruct Alexa "delete what I [just said][said today]."

Auto Delete Old Recordings - Follow the same instructions but choose Manage Your Alexa Data and set auto delete to either after 3 or 18 months.

Turn Off "Use Voice Recordings to Improve Amazon Services" - Again, using the same

Article

NEWS

The People vs. Amazon Alexa: Connected Devices Are Not Hostile Witnesses

Share

Create PDF

Christopher B. Hopkins | Wednesday, November 4, 2020

McDonald Hopkins member Christopher B. Hopkins recently had an article published by The American Bar Association.

Article

TECHNOLOGY Corner

Is Your PC Keeping Your Information Private? Take This 10-Question Quiz

CHRISTOPHER B. HOPKINS

What entity was the victim of the largest data breach in history? According to *The Guardian,* the "biggest [hack] in history" involved 11.5 million documents known as the Panama Papers stolen from... a law firm. "BigLaw" firms are not alone – small firms and solo lawyers frequently suffer ransomware attacks while, according to Verizon, in-house lawyers are, "far more likely to actually open a [phishing] email than all other [corporate] departments." Lawyers are particularly susceptible targets for data breach because we often hold clients' confidential and financial information. Worse, we can be a weak link: lawyers are quick to answer client inquiries and we respond quickly and at all hours from our mobile devices.

new software. Unless it is a personal computer, few users need full "admin rights." Tap the Windows key and type "control panel." Select User Accounts (twice). 5 points if "administrator" does not appear under your name. If it says "administrator," and it is not your personal PC, subtract 5 points.

4. Is Your Hard Drive Encrypted? An encrypted drive should render your drive unreadable if it is stolen. Tap the Windows key and type "control panel." Select "Security and Systems" and look for BitLocker encryption to be "on." Admittedly, there is more than one encryption method; hit the Windows key and type "PGP" to see if you find PGP Whole Disk Encryption. 5 points for encryption, no points for an

8. Can Someone Else Remotely Access my PC? Hit the Windows key and R, then type "SystemPropertiesRemote.exe." It should open a new dialog box with the title "Remote Access." If "Allow Remote Assistance" is unchecked, give yourself 5 points. If your IT department allows remote access limited to "Network Level Authentication," add no points. If remote access is allowed without restriction, subtract 5 points.

9. Do I Have Any Unknown Programs on my PC? Tap the Windows key and type "control panel." In the upper right corner, type, "program" in the search box, and select "show which programs are installed." Add 3 points if you recognize all apps; -1 for each app you cannot identify.

Click for full article

TECHNOLOGY CORNER

CHRISTOPHER B. HOPKINS

Protect The Privacy of Your iOS 13 Device

It has been two years since we covered iPhone and iPad security in this column. The risks have only increased while several privacy settings have become more difficult to find. To echo the Fourth District's recent assessment in a real-time cell phone tracking case: "[t]his presents significant privacy concerns." Make sure your device is running iOS 13.x (Settings / General / Software Update) and then check the following:

Apple Is Tracking You: Under Settings / Privacy / Location Services, scroll all the way down to System Services. Location-Based Apple Ads, Location-Based Suggestions, iPhone Analytics, Popular Near Me, and Routing & Traffic should be off. Turn off Significant Locations.

Google Maps Is Tracking You: Open Google Maps and select your profile in the upper

prevent this intrusion, go to Settings / Mail and toggle Load Remote Images to off. If an email contains an image you want to see, just click the banner at the top when you open the email.

I See When You Opened My Text: Under Settings / Messages, turn off "Send Read Receipts."

I See You Are Not in Your Office: Why broadcast that you are out of the office? Turn off "sent from my iPhone" under Settings / Mail / Signatures (leave it blank). There is still another trick. When sending a reply, your email will be entitled "Re:" when you reply on a mobile device whereas it will be "RE," with a capital E, if you are logged in via computer. So an email which is entitled, "Re: [title]" is coming from a handheld device. When it matters, you can manually capitalize the letter "e" to prevent leaking

able to keylog what you type because you granted them "all access." Make sure you know which apps can read your texts under General / Keyboard / Keyboards. Delete anything which is unfamiliar.

Are Text Messages Going to Other Devices? Are iMessages being pushed to other devices on your Apple account? Maybe. To keep your chats private, make sure Settings / Messages / Send & Receive is set to your phone only and no other devices or email.

Health: Unless you intended an app to access this feature, only Health should be listed under Settings / Health / Data.

---

*Christopher B. Hopkins handles privacy and cybersecurity matters with McDonald Hopkins LLC (**chopkins@mcdonaldhopkins.com**).*

Click for full article

CHRISTOPHER B. HOPKINS

McDonald Hopkins

CHOPKINS@MCDONALDHOPKINS.COM

@cbhopkins www.linkedin.com/in/cbhopkins/

InternetLawCommentary.com