E-DISCOVERY: MOBILE DEVICES AND SOCIAL MEDIA IN E-DISCOVERY

PROGRAM MATERIALS

March 28, 2018
E-DISCOVERY:
MOBILE DEVICES AND SOCIAL MEDIA IN E-DISCOVERY

2.5 CLE Hours Including
1 Trial Practice Hour

Sponsored By: Institute of Continuing Legal Education
Copyright © 2018 by the Institute of Continuing Legal Education of the State Bar of Georgia. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise, without the prior written permission of ICLE.

The Institute of Continuing Legal Education’s publications are intended to provide current and accurate information on designated subject matter. They are offered as an aid to practicing attorneys to help them maintain professional competence with the understanding that the publisher is not rendering legal, accounting, or other professional advice. Attorneys should not rely solely on ICLE publications. Attorneys should research original and current sources of authority and take any other measures that are necessary and appropriate to ensure that they are in compliance with the pertinent rules of professional conduct for their jurisdiction.

ICLE gratefully acknowledges the efforts of the faculty in the preparation of this publication and the presentation of information on their designated subjects at the seminar. The opinions expressed by the faculty in their papers and presentations are their own and do not necessarily reflect the opinions of the Institute of Continuing Legal Education, its officers, or employees. The faculty is not engaged in rendering legal or other professional advice and this publication is not a substitute for the advice of an attorney. This publication was created to serve the continuing legal education needs of practicing attorneys.

ICLE does not encourage non-attorneys to use or purchase this publication in lieu of hiring a competent attorney or other professional. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

Although the publisher and faculty have made every effort to ensure that the information in this book was correct at press time, the publisher and faculty do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

The Institute of Continuing Legal Education of the State Bar of Georgia is dedicated to promoting a well organized, properly planned, and adequately supported program of continuing legal education by which members of the legal profession are afforded a means of enhancing their skills and keeping abreast of developments in the law, and engaging in the study and research of the law, so as to fulfill their responsibilities to the legal profession, the courts and the public.
SOLACE is a program of the State Bar of Georgia designed to assist those in the legal community who have experienced some significant, potentially life-changing event in their lives. SOLACE is voluntary, simple and straightforward. SOLACE does not solicit monetary contributions but accepts assistance or donations in kind.

Contact SOLACE@gabar.org for help.

**Who are we?**

**SOLACE** is a program of the State Bar of Georgia designed to assist those in the legal community who have experienced some significant, potentially life-changing event in their lives. SOLACE is voluntary, simple and straightforward. SOLACE does not solicit monetary contributions but accepts assistance or donations in kind.

**How does SOLACE work?**

If you or someone in the legal community is in need of help, simply email SOLACE@gabar.org. Those emails are then reviewed by the SOLACE Committee. If the need fits within the parameters of the program, an email with the pertinent information is sent to members of the State Bar.

**What needs are addressed?**

Needs addressed by the SOLACE program can range from unique medical conditions requiring specialized referrals to a fire loss requiring help with clothing, food or housing. Some other examples of assistance include gift cards, food, meals, a rare blood type donation, assistance with transportation in a medical crisis or building a wheelchair ramp at a residence.
The purpose of the SOLACE program is to allow the legal community to provide help in meaningful and compassionate ways to judges, lawyers, court personnel, paralegals, legal secretaries and their families who experience loss of life or other catastrophic illness, sickness or injury.

**TESTIMONIALS**

In each of the Georgia SOLACE requests made to date, Bar members have graciously stepped up and used their resources to help find solutions for those in need.

A solo practitioner’s quadriplegic wife needed rehabilitation, and members of the Bar helped navigate discussions with their insurance company to obtain the rehabilitation she required.

A Louisiana lawyer was in need of a CPAP machine, but didn’t have insurance or the means to purchase one. Multiple members offered to help.

A Bar member was dealing with a serious illness and in the midst of brain surgery, her mortgage company scheduled a foreclosure on her home. Several members of the Bar were able to negotiate with the mortgage company and avoided the pending foreclosure.

Working with the South Carolina Bar, a former paralegal’s son was flown from Cyprus to Atlanta (and then to South Carolina) for cancer treatment. Members of the Georgia and South Carolina bars worked together to get Gabriel and his family home from their long-term mission work.

Contact SOLACE@gabar.org for help.
Dear ICLE Seminar Attendee,

Thank you for attending this seminar. We are grateful to the Chairperson(s) for organizing this program. Also, we would like to thank the volunteer speakers. Without the untiring dedication and efforts of the Chairperson(s) and speakers, this seminar would not have been possible. Their names are listed on the AGENDA page(s) of this book, and their contributions to the success of this seminar are immeasurable.

We would be remiss if we did not extend a special thanks to each of you who are attending this seminar and for whom the program was planned. All of us at ICLE hope your attendance will be beneficial as well as enjoyable. We think that these program materials will provide a great initial resource and reference for you.

If you discover any substantial errors within this volume, please do not hesitate to inform us. Should you have a different legal interpretation/opinion from the speaker’s, the appropriate way to address this is by contacting him/her directly.

Your comments and suggestions are always welcome.

Sincerely,
Your ICLE Staff

*Jeffrey R. Davis*
Executive Director, State Bar of Georgia

*Tangela S. King*
Director, ICLE

*Rebecca A. Hall*
Associate Director, ICLE
Presiding:
Rachael L. Zichella, Program Co-chair, Taylor English Duma LLP, Atlanta
Scott P. Hilsen, Program Co-chair, KPMG LLP, Atlanta

7:30 REGISTRATION AND CONTINENTAL BREAKFAST (All attendees must check in upon arrival. A jacket or sweater is recommended.)

8:00 WELCOME

8:10 BYOD (BRING YOUR OWN DEVICE) AND SEDONA CONFERENCE COMMENTARY
Rachael L. Zichella

8:30 PANEL: DATA ON DEVICES AND IN SOCIAL MEDIA – WHAT’S OUT THERE AND HOW TO GET IT
Johnny Lee, Principal, Grant Thornton, Atlanta
Jay Ferro, Global Chief Information & Technology Officer, TransPerfect, Atlanta
Anthony DeSarro, Manager Forensic Technology, KPMG, Atlanta

9:30 BREAK

9:45 PANEL: E-DISCOVERY ISSUES AND PRACTICES WITH DEVICES AND SOCIAL MEDIA
Stephanie O. Mitchell, Litigation Counsel, Siemens Corporation, Alpharetta
Allison A. Grounds, Managing Director, Troutman Sanders eMerge, Troutman Sanders LLP, Atlanta
Scott A. Wandstrat, Partner, Arnall Golden Gregory LLP, Atlanta

11:00 ADJOURN
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>V</td>
</tr>
<tr>
<td>Agenda</td>
<td>VII</td>
</tr>
<tr>
<td>E-Discovery: Mobile Devices and Social Media in E-Discovery</td>
<td>9-60</td>
</tr>
<tr>
<td>Appendix:</td>
<td></td>
</tr>
<tr>
<td>ICLE Board</td>
<td>1</td>
</tr>
<tr>
<td>Georgia Mandatory CLE Fact Sheet</td>
<td>2</td>
</tr>
</tbody>
</table>
8:10  BYOD (BRING YOUR OWN DEVICE) AND SEDONA CONFERENCE COMMENTARY
Rachael L. Zichella
More than ever before, organizations are permitting or encouraging workers to use their own personal devices to access, create, and manage the organization’s information—often after hours and outside the office. This practice is commonly referred to as Bring Your Own Device or BYOD, and is often accomplished through a BYOD program that includes formal or informal rules and guidelines. The Commentary on BYOD is designed to help organizations develop and implement workable—and legally defensible—BYOD policies and practices. The commentary also addresses how creating and storing an organization’s information on devices owned by employees impacts the organization’s discovery obligations.

The first two principles and related commentary address determining whether a BYOD program is the right choice for an organization, followed by basic information governance requirements for BYOD—security, privacy, accessibility, and disposition—from the perspective of both domestic and global organizations. Against this backdrop, the remaining principles and commentary address preparing for and responding to discovery obligations under the prevailing U.S. approach to discovery.

**Principle 1:** Organizations should consider their business needs and objectives, their legal rights and obligations, and the rights and expectations of their employees when deciding whether to allow, or even require, BYOD.

**Principle 2:** An organization’s BYOD program should help achieve its business objectives while also protecting both business and personal information from unauthorized access, disclosure, and use.

**Principle 3:** Employee-owned devices that contain unique, relevant ESI should be considered sources for discovery.

**Principle 4:** An organization’s BYOD policy and practices should minimize the storage of—and facilitate the preservation and collection of—unique, relevant ESI from BYOD devices.

**Principle 5:** Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery.
The Sedona Conference

Please note that this version of the Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations is open for public comment through March 26, 2018, and suggestions for improvement are very welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please submit comments by email to comments@sedonaconference.org.

The full text of The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary%20on%20BYOD.
8:30  PANEL: DATA ON DEVICES AND IN SOCIAL MEDIA – WHAT’S OUT THERE AND HOW TO GET IT

Johnny Lee, Principal, Grant Thornton, Atlanta
Jay Ferro, Global Chief Information & Technology Officer, TransPerfect, Atlanta
Anthony DeSarro, Manager Forensic Technology, KPMG, Atlanta
What is a mobile device?
They can be big...

They can be small...
They can take many forms...

What is a mobile device?

- **According to NIST**:
  - “Mobile device features are constantly changing, so it is difficult to define the term mobile device.”
- **Hardware and Software characteristics**:
  - A small form factor
  - At least one wireless network interface for network access (data communications) – Wi-Fi, Cellular, Bluetooth, or other connection technology
  - Local built-in data storage
  - An operating system that is not a full-fledged desktop or laptop operating system
  - Applications available through multiple methods
What are mobile devices used for?

- No longer solely used for phone calls. They are full blown computers!
  - Phone calls
  - Texting (SMS, MMS)
  - Chatting (Text/Video)
  - Camera
  - Social media
  - Web Browser
  - Entertainment
  - Email
  - Productivity
  - Calendar
  - Contacts
  - Games
  - Navigation
  - Application usage
Where can mobile data be found?

- SIM Card
- Internal Mobile Storage
- External Mobile Storage – SD Card
- Backups stored on computers
- Backups stored in the cloud
- Mobile service provider data
  - Tower info, call records
- Cloud

- Remember, mobile information may not ONLY be located on the device itself.
GM - Ignition Switch Case Dismissed

- Robert Scheuer, a postal worker, claimed an ignition switch flaw disabled his airbag in an auto accident.
- Blamed GM for his family’s eviction from their “dream house.”
- He had asked his real estate agent if he could move into the house early. His agent said he would need proof of funds – showing he could afford the home.
- Robert provided a text message with a photo of his retirement stub.
- On the strength of that stub, the real estate agent had let Mr. Scheuer and his wife, Lisa, move in to the new house before they had paid for it.
- He was soon after evicted from the home. He argued that memory loss, as a result of the accident, caused him to misplace a $49,500 check for a down payment on the home.
- During the middle of the trial, GM received a tip from Mr. Scheuer’s former real estate agent.
- The real estate agent stated that the Scheuer family was evicted from the home because Mr. Scheuer faked the stub from his retirement fund that was used for “proof of funds” to close the sale.
- According to the agent, Mr. Scheuer had altered a government check stub to make it look like he had hundreds of thousands of dollars in the bank.
- The real estate agent said he had to evict them when he learned that the check was fraudulent – “441” was added to the $430.72 stub to turn it into a deposit of $441,430.72.
- The judge notably remarked to the attorneys that the check stub “appears quite clearly to my mind to have been doctored.”
Rules

• The answer is – it depends.
• Turning OFF a device could prevent you from ever accessing it again.
  • Encryption
  • Failure to have the proper pin/passcode/pattern to log into the device.
• Failing to turn OFF a device or failing to isolate it from networks could allow for the destruction of evidence.
  • Users can issue remote wiping commands.
  • Some phones have an automatic timer to turn on the phone for updates, which could compromise data, so battery removal may be necessary.
  • Some phones will perform automatic cleanup routines.
• Turning ON a device when it is off will cause changes to the device.
  • Unlike forensic collections of hard drives (where we can collect an image of the drive without making any changes), in some cases, we must turn ON the device and enable features in order to capture an image.
• Some common protection measures that are often used include: disabling Wi-Fi, disabling Bluetooth, enabling airplane mode, and the use of faraday bags to isolate networks or access to the device.

Reminder

• Mobile devices can include trace evidence, DNA, and fingerprints.
• Some corporate security policies on mobile devices can cause issues or prevent our forensic tools from supporting the device.
• A dead person’s finger might still work at opening a locked phone.
• SD cards might be unencrypted, partial encrypted, or fully encrypted.
• Most smartphones will embed EXIF information in photos and videos.
Lettuce talk about EXIF

- User anonymously posts on 4chan bulletin board: "This is the lettuce you eat at Burger King."
- The original post went live on July 16 at 11:38 p.m.
- At 11:47 p.m., another 4chan user noted that the photo's Exif data pointed to Mayfield Heights, Ohio.
- At 11:50 p.m., just 12 minutes later, someone posted the address of the Burger King branch in which the lettuce-stepping occurred.
- At 11:55 p.m., someone contacted the news.
- At 11:58 p.m., someone posted the link to Burger King's Tell Us About Us form, with the photo attached.
- The next morning, Cleveland Scene Magazine contacted the Burger King establishment and talked to the breakfast shift manager, who, upon seeing the offending photo, said "Oh, I know who that is. He's getting fired."

EXIF Provides Body of Evidence

- A hacker hacked into US law enforcement agencies and released phone numbers and home addresses of police officers.
- You're looking at the evidence the FBI used to catch him. →
- This is his girlfriend.
- EXIF showed that the photo was taken at the woman's home.
EXIF - Hide your wife, hide your kids

EXIF Used to Attack US Helicopters

- New fleet of helicopters arrived at a base in Iraq.
- Some soldiers took pictures and posted to the Internet.
- The enemy used EXIF information to identify the exact location of the helicopters inside the compound and conducted a mortar attack.
- Destroyed four of the helicopters.
Boston Bombing EXIF

- April, 15, 2013 – Two bomb blasts tore through a crowd of people watching runners approaching the finish line.
- Within 24hrs, the FBI had amassed more than 10 terabytes of data through crowd sourcing.

How do we collect mobile devices?
Can we collect from all mobile devices?

- No, in some cases we can’t leverage our standard forensic imaging tools to automate or speed up the capture of a device.
- Make/Model may be too new.
- Make/Model may be unsupported.
- Make/Model old (older flip phones).
- Even OS upgrades can cause issues.

What can we collect?

- Phone call logs
- Texts (SMS, MMS)
- Chats
- Social media records
- Web Browser activity
- Media Files (Pictures, Video)
- Email
- Calendar
- Contacts
- GPS locations
- List of installed applications
- IP addresses
- Searched items
- User accounts
- User Dictionary
- Web History
- Wireless Networks
- Databases
- Carved for data
- Application information/databases
- All dependent on the make/model/OS/type of collection/level of support of our forensic tools/permissions to the device, etc.
- And more!
The Internet of Things (IoT) Defined

“The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.”

Recent DYN attack

• On October 21, 2016, there was multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn which made major Internet platforms and services unavailable to large swaths of users in Europe and North America.

• As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address.

• The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses.

• The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devices—such as printers, cameras, residential gateways and baby monitors—that had been infected with the Mirai malware.

• With an estimated load of 1.2 terabits per second, the attack was, according to experts, the largest DDoS on record.

• https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
Continuous Positive Airway Pressure

- Modem
- Bluetooth
- SD Card
- Mobile App on my phone

Fitbit Data Used in Court

- In Lancaster, Pennsylvania cops responded to a 911 call by a woman who claimed she was sexually assaulted.
- The woman told the police she woke up around midnight with the stranger on top of her.
- Authorities found her Fitbit, which recorded her as active, awake and walking around all night.
- Combined with the evidence that was missing (tracks outside in the snow from boots she said the attacker was wearing, or any sign of them inside), an investigation led to her facing misdemeanor charges.

Source:
Another Fitbit case...

- A Canadian law firm will use data from a Fitbit fitness tracker for the first time in court as an objective measure of activity.
- The data will be provided by the plaintiff in a personal injury lawsuit in an effort to show life-affecting reduced activity post injury.
- The lawyers aren’t using Fitbit’s data directly, but pumping it through analytics platform Vivametrica, which uses public research to compare a person’s activity data with that of the general population.
- Future: Could see insurance companies insisting that claimants undergo assessment via fitness tracker.

Source:

Suri: “I need to hide my roommate”

- During the trial of Pedro Bravo, who is charged with kidnapping, strangling and murdering his friend Christian Aguilar, prosecutors showed evidence that he had a photo of a Siri search that said, “I need to hide my roommate.”
- While some media outlets reported that the question was asked by Bravo on the day Aguilar disappeared — Gainesville Police Department now says otherwise.
- Image was actually in Facebook Cache.
- The defendant also had an iPhone 4 and Siri wasn’t available until the 4S.
- He had Verizon, but the screenshot showed AT&T.
- Officer Goeckel did find GPS data that allegedly contradicts Bravo’s stated whereabouts at the time of Aguilar’s death. He also turned his cellular connection off for an hour in the middle of that night, and his flashlight app had been used for 48 minutes that day.
Snapchat

- Christal McGee was allegedly using Snapchat while driving 100 miles per hour
- Maynard (person she hit) is suing McGee & Snapchat
- Maynard had serious injuries and brain damage
- She denies using Snapchat before the crash
- She posted a Snap of her injuries

- Question: Was she on the app at the time?

Pokémon GO

The graph shows the number of Pokémon GO users in the United States as of July 2016. Shortly after its release, the game had 21 million daily active users in the U.S. and the user numbers peaked on July 19, reaching 45 million.

Source: Statista (pulled on 11/2/2016)
Pokémon GO

- A teen was tragically shot dead on Sunday after trespassing onto private property while attempting to catch a Pokémon in the new game “Pokémon Go”.

- Blames Pokémon Go for taking her across a busy intersection

Time Card Submission Investigation

Did John actually work 8hrs? The more data points, the better!
Why are all these things important?

- More data points we have, the better we can answer the:
  - Who
  - What
  - Where
  - When
  - Why
- Data provides us some very useful information that you might not otherwise have: timestamps, locations, etc.
- Fill in our investigative timelines.
Jeep Hacked!
App Usage

<table>
<thead>
<tr>
<th>Mobile App Usage Overview</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of mobile apps downloads worldwide</td>
<td>102.062m</td>
</tr>
<tr>
<td>Projected number of apps downloads 2017</td>
<td>268.692m</td>
</tr>
<tr>
<td>Number of free mobile apps downloads</td>
<td>92.888bn</td>
</tr>
<tr>
<td>Number of paid mobile app downloads</td>
<td>9.198bn</td>
</tr>
<tr>
<td>Worldwide mobile app revenue</td>
<td>$41.1bn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>App Stores</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of apps available in Google Play store</td>
<td>2,200,000</td>
</tr>
<tr>
<td>Number of apps available in Windows Store</td>
<td>649,000</td>
</tr>
<tr>
<td>Number of cumulative downloads from Apple App Store</td>
<td>140bn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reach &amp; Traffic</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique U.S. visitors to Facebook app on iOS</td>
<td>47.25m</td>
</tr>
<tr>
<td>Number of unique U.S. visitors to Google Play app on Android</td>
<td>72.25m</td>
</tr>
<tr>
<td>Monthly social media minutes spent on Facebook in U.S.</td>
<td>230</td>
</tr>
</tbody>
</table>

Source: Statista (pulled on 11/2/2016)

Monthly mobile app usage frequency as of 4th quarter 2015, by category

Monthly mobile app usage frequency as of 4th quarter 2015, by category

The statistic represents the average monthly app usage frequency of selected app categories as of the fourth quarter of 2015. E-commerce and retail apps were at the top of the frequency engagement list with an average of 17.5 sessions per month.

Source: Statista (pulled on 11/2/2016)
Most popular mobile apps in the United States as of July 2016, ranked by average unique monthly visitors (in millions)

- Facebook: 149.00
- Facebook Messenger: 131.51
- YouTube: 115.35
- Google Maps: 100.85
- Google Search: 80.26
- Google Play: 88.63
- Netflix: 80.46
- Pandora: 74.78
- Instagram: 73.55
- Amazon Mobile: 71.42
- Apple Music: 63
- Apple Maps: 62.96
- Pokémon Go: 54.54
- Snapchat: 54.31
- Pinterest: 51.29

This statistic gives information on the most popular mobile apps in the United States as of July 2016, ranked by average unique monthly visitors on iOS and Android platforms.

Source: Statista (pulled on 11/2/2016)

BYOD (Bring Your Own Device)

Pro: Cheaper for company
Cons: Complicates eDiscovery for litigation matters and investigations
No centralized password management.
Make sure you have the proper policies and approvals in place.
Who owns the device might dictate if you can even touch it.
You might need to gather written consent.
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.
9:45  PANEL: E-DISCOVERY ISSUES AND PRACTICES WITH DEVICES AND SOCIAL MEDIA  
Stephanie O. Mitchell, Litigation Counsel, Siemens Corporation, Alpharetta  
Allison A. Grounds, Managing Director, Troutman Sanders eMerge, Troutman Sanders LLP, Atlanta  
Scott A. Wandstrat, Partner, Arnall Golden Gregory LLP, Atlanta
DIFIORE, Chief Judge:

In this personal injury action, we are asked to resolve a dispute concerning disclosure of materials from plaintiff’s Facebook account.

Plaintiff alleges that she was injured when she fell from a horse owned by defendant, suffering spinal and traumatic brain injuries resulting in cognitive deficits, memory loss,
difficulties with written and oral communication, and social isolation. At her deposition, plaintiff stated that she previously had a Facebook account on which she posted “a lot” of photographs showing her pre-accident active lifestyle but that she deactivated the account about six months after the accident and could not recall whether any post-accident photographs were posted. She maintained that she had become reclusive as a result of her injuries and also had difficulty using a computer and composing coherent messages. In that regard, plaintiff produced a document she wrote that contained misspelled words and faulty grammar in which she represented that she could no longer express herself the way she did before the accident. She contended, in particular, that a simple email could take hours to write because she had to go over written material several times to make sure it made sense.

Defendant sought an unlimited authorization to obtain plaintiff’s entire “private” Facebook account, contending the photographs and written postings would be material and necessary to his defense of the action under CPLR 3101(a). When plaintiff failed to provide the authorization (among other outstanding discovery), defendant moved to compel, asserting that the Facebook material sought was relevant to the scope of plaintiff’s injuries and her credibility. In support of the motion, defendant noted that plaintiff alleged that she was quite active before the accident and had posted photographs on Facebook reflective of that fact, thus affording a basis to conclude her Facebook account would contain evidence relating to her activities. Specifically, defendant cited the claims that plaintiff can no longer cook, travel, participate in sports, horseback ride, go to the movies, attend the theater, or go boating, contending that photographs and messages she posted on
Facebook would likely be material to these allegations and her claim that the accident negatively impacted her ability to read, write, word-find, reason and use a computer.

Plaintiff opposed the motion arguing, as relevant here, that defendant failed to establish a basis for access to the “private” portion of her Facebook account because, among other things, the “public” portion contained only a single photograph that did not contradict plaintiff’s claims or deposition testimony. Plaintiff’s counsel did not affirm that she had reviewed plaintiff’s Facebook account, nor allege that any specific material located therein, although potentially relevant, was privileged or should be shielded from disclosure on privacy grounds. At oral argument on the motion, defendant reiterated that the Facebook material was reasonably likely to provide evidence relevant to plaintiff’s credibility, noting for example that the timestamps on Facebook messages would reveal the amount of time it takes plaintiff to write a post or respond to a message. Supreme Court inquired whether there is a way to produce data showing the timing and frequency of messages without revealing their contents and defendant acknowledged that it would be possible for plaintiff to turn over data of that type, although he continued to seek the content of messages she posted on Facebook.

Supreme Court granted the motion to compel to the limited extent of directing plaintiff to produce all photographs of herself privately posted on Facebook prior to the accident that she intends to introduce at trial, all photographs of herself privately posted on Facebook after the accident that do not depict nudity or romantic encounters, and an authorization for Facebook records showing each time plaintiff posted a private message after the accident and the number of characters or words in the messages. Supreme Court
did not order disclosure of the content of any of plaintiff’s written Facebook posts, whether authored before or after the accident.

Although defendant was denied much of the disclosure sought in the motion to compel, only plaintiff appealed to the Appellate Division.1 On that appeal, the court modified by limiting disclosure to photographs posted on Facebook that plaintiff intended to introduce at trial (whether pre- or post-accident) and eliminating the authorization permitting defendant to obtain data relating to post-accident messages, and otherwise affirmed. Two Justices dissented, concluding defendant was entitled to broader access to plaintiff’s Facebook account and calling for reconsideration of that court’s recent precedent addressing disclosure of social media information as unduly restrictive and inconsistent with New York’s policy of open discovery. The Appellate Division granted defendant leave to appeal to this Court, asking whether its order was properly made. We reverse, reinstate Supreme Court’s order and answer that question in the negative.

Disclosure in civil actions is generally governed by CPLR 3101(a), which directs: “[t]here shall be full disclosure of all matter material and necessary to the prosecution or defense of an action, regardless of the burden of proof.” We have emphasized that “[t]he words ‘material and necessary,’ . . . are to be interpreted liberally to require disclosure,

1 Defendant’s failure to appeal Supreme Court’s order impacts the scope of his appeal in this Court. “Our review of [an] Appellate Division order is ‘limited to those parts of the [order] that have been appealed and that aggrieve the appealing party’” (Hain v Jamison, 28 NY3d 524, 534 [2016], quoting Hecht v City of New York, 60 NY2d 57 [1983]). Because defendant did not cross-appeal and, thus, sought no affirmative relief from the Appellate Division, he is aggrieved by the Appellate Division order only to the extent it further limited Supreme Court’s disclosure order.
upon request, of any facts bearing on the controversy which will assist preparation for trial by sharpening the issues and reducing delay and prolixity. The test is one of usefulness and reason” (Allen v Crowell-Collier Publ. Co., 21 NY2d 403, 406 [1968]; see also Andon v 302-304 Mott St. Assoc., 94 NY2d 740, 746 [2000]). A party seeking discovery must satisfy the threshold requirement that the request is reasonably calculated to yield information that is “material and necessary” – i.e., relevant – regardless of whether discovery is sought from another party (see CPLR 3101[a][1]) or a nonparty (CPLR 3101[a][4]; see e.g. Matter of Kapon v Koch, 23 NY3d 32 [2014]). The “statute embodies the policy determination that liberal discovery encourages fair and effective resolution of disputes on the merits, minimizing the possibility for ambush and unfair surprise” (Spectrum Systems Intern. Corp. v Chemical Bank, 78 NY2d 371, 376 [1991]).

The right to disclosure, although broad, is not unlimited. CPLR 3101 itself “establishes three categories of protected materials, also supported by policy considerations: privileged matter, absolutely immune from discovery (CPLR 3101[b]); attorney’s work product, also absolutely immune (CPLR 3101[c]); and trial preparation materials, which are subject to disclosure only on a showing of substantial need and undue hardship” (Spectrum, supra, at 377). The burden of establishing a right to protection under these provisions is with the party asserting it – “the protection claimed must be narrowly construed; and its application must be consistent with the purposes underlying the immunity” (id.).

In addition to these restrictions, this Court has recognized that “litigants are not without protection against unnecessarily onerous application of the disclosure statutes.
Under our discovery statutes and case law competing interests must always be balanced; the need for discovery must be weighed against any special burden to be borne by the opposing party” (Kavanaugh v Ogden Allied Maintenance Corp., 92 NY2d 952, 954 [1998] [citations and internal quotation marks omitted]; see CPLR 3103[a]). Thus, when courts are called upon to resolve a dispute, discovery requests “must be evaluated on a case-by-case basis with due regard for the strong policy supporting open disclosure . . . Absent an [error of law or an] abuse of discretion, this Court will not disturb such a determination (Andon, supra, 94 NY2d at 747; see Kavanaugh, supra, 92 NY2d at 954).3

Here, we apply these general principles in the context of a dispute over disclosure of social media materials. Facebook is a social networking website “where people can share information about their personal lives, including posting photographs and sharing

2 While courts have the authority to oversee disclosure, by design the process often can be managed by the parties without judicial intervention. If the party seeking disclosure makes a targeted demand for relevant, non-privileged materials (see CPLR 3120[1][i], [2] [permitting a demand for items within the other party’s “possession, custody or control,” which “shall describe each item and category with reasonable particularity”]), counsel for the responding party – after examining any potentially responsive materials – should be able to identify and turn over items complying with the demand. Attorneys, while functioning as advocates for their clients’ interests, are also officers of the court who are expected to make a bona fide effort to properly meet their obligations in the disclosure process. When the process is functioning as it should, there is little need for a court in the first instance to winnow the demand or exercise its in camera review power to cull through the universe of potentially responsive materials to determine which are subject to discovery.

3 Further, the Appellate Division has the power to exercise independent discretion – to substitute its discretion for that of Supreme Court, even when it concludes Supreme Court’s order was merely improvident and not an abuse of discretion – and when it does so applying the proper legal principles, this Court will review the resulting Appellate Division order under the deferential “abuse of discretion” standard (see e.g. Andon, supra; Kavanaugh, supra; see generally Kapon, supra).
information about what they are doing or thinking” (Romano v Steelcase, Inc., 30 Misc 3d 426 [Sup Ct Suffolk County 2010]). Users create unique personal profiles, make connections with new and old “friends” and may “set privacy levels to control with whom they share their information” (id.). Portions of an account that are “public” can be accessed by anyone, regardless of whether the viewer has been accepted as a “friend” by the account holder – in fact, the viewer need not even be a fellow Facebook account holder (see Facebook Help: What audiences can I choose from when I share? https://www.facebook.com/help/211513702214269?helpref=faq_content [last accessed January 15, 2018]). However, if portions of an account are “private,” this typically means that items are shared only with “friends” or a subset of “friends” identified by the account holder (id.). While Facebook – and sites like it – offer relatively new means of sharing information with others, there is nothing so novel about Facebook materials that precludes application of New York’s long-standing disclosure rules to resolve this dispute.

On appeal in this Court, invoking New York’s history of liberal discovery, defendant argues that the Appellate Division erred in employing a heightened threshold for production of social media records that depends on what the account holder has chosen to share on the public portion of the account. We agree. Although it is unclear precisely what standard the Appellate Division applied, it cited its prior decision in Tapp v New York State Urban Dev. Corp. (102 AD3d 620 [1st Dept 2013]), which stated: “To warrant discovery, defendants must establish a factual predicate for their request by identifying relevant information in plaintiff’s Facebook account – that is, information that ‘contradicts or conflicts with plaintiff’s alleged restrictions, disabilities, and losses, and other claims’”
Several courts applying this rule appear to have conditioned discovery of material on the “private” portion of a Facebook account on whether the party seeking disclosure demonstrated there was material in the “public” portion that tended to contradict the injured party’s allegations in some respect (see e.g. Spearin v Linmar, 129 AD3d 528 [1st Dept 2015]; Nieves v 30 Ellwood Realty LLC, 39 Misc 3d 63 [App Term 2013]; Pereira v City of New York, 40 Misc 3d 1210[A] [Sup Ct Queens County 2013]; Romano, supra, 30 Misc 3d 426). Plaintiff invoked this precedent when arguing, in opposition to the motion to compel, that defendant failed to meet the minimum threshold permitting discovery of any Facebook materials.

Before discovery has occurred – and unless the parties are already Facebook “friends” – the party seeking disclosure may view only the materials the account holder happens to have posted on the public portion of the account. Thus, a threshold rule requiring that party to “identify relevant information in [the] Facebook account” effectively permits disclosure only in limited circumstances, allowing the account holder to unilaterally obstruct disclosure merely by manipulating “privacy” settings or curating the materials on the public portion of the account.4 Under such an approach, disclosure turns

\[
\text{id. at 620 [emphasis added]}. \]  

4 This rule has been appropriately criticized by other courts. As one federal court explained, “[t]his approach can lead to results that are both too broad and too narrow. On the one hand, a plaintiff should not be required to turn over the private section of his or her Facebook profile (which may or may not contain relevant information) merely because the public section undermines the plaintiff’s claims. On the other hand, a plaintiff should be required to review the private section and produce any relevant information, regardless of what is reflected in the public section . . . Furthermore, this approach shields from discovery the information of Facebook users who do not share any information publicly” (Giacchetto v Patchogue-Medford Union Free School Dist., 293 FRD 112, 114 [ED NY 2013]).
on the extent to which some of the information sought is already accessible – and not, as it should, on whether it is “material and necessary to the prosecution or defense of an action” (see CPLR 3101[a]).

New York discovery rules do not condition a party’s receipt of disclosure on a showing that the items the party seeks actually exist; rather, the request need only be appropriately tailored and reasonably calculated to yield relevant information. Indeed, as the name suggests, the purpose of discovery is to determine if material relevant to a claim or defense exists. In many if not most instances, a party seeking disclosure will not be able to demonstrate that items it has not yet obtained contain material evidence. Thus, we reject the notion that the account holder’s so-called “privacy” settings govern the scope of disclosure of social media materials.

That being said, we agree with other courts that have rejected the notion that commencement of a personal injury action renders a party’s entire Facebook account automatically discoverable (see e.g. Kregg v Maldonado, 98 AD3d 1289, 1290 [4th Dept 2012] [rejecting motion to compel disclosure of all social media accounts involving injured party without prejudice to narrowly-tailored request seeking only relevant information]; Giacchetto, supra, 293 FRD 112, 115; Kennedy v Contract Pharmacal Corp., 2013 WL 1966219, *2 [ED NY 2013]). Directing disclosure of a party’s entire Facebook account is comparable to ordering discovery of every photograph or communication that party shared with any person on any topic prior to or since the incident giving rise to litigation – such an order would be likely to yield far more nonrelevant than relevant information. Even
under our broad disclosure paradigm, litigants are protected from “unnecessarily onerous application of the discovery statutes” (Kavanaugh, supra, 92 NY2d at 954).

Rather than applying a one-size-fits-all rule at either of these extremes, courts addressing disputes over the scope of social media discovery should employ our well-established rules – there is no need for a specialized or heightened factual predicate to avoid improper “fishing expeditions.” In the event that judicial intervention becomes necessary, courts should first consider the nature of the event giving rise to the litigation and the injuries claimed, as well as any other information specific to the case, to assess whether relevant material is likely to be found on the Facebook account. Second, balancing the potential utility of the information sought against any specific “privacy” or other concerns raised by the account holder, the court should issue an order tailored to the particular controversy that identifies the types of materials that must be disclosed while avoiding disclosure of nonrelevant materials. In a personal injury case such as this it is appropriate to consider the nature of the underlying incident and the injuries claimed and to craft a rule for discovering information specific to each. Temporal limitations may also be appropriate – for example, the court should consider whether photographs or messages posted years before an accident are likely to be germane to the litigation. Moreover, to the extent the account may contain sensitive or embarrassing materials of marginal relevance, the account holder can seek protection from the court (see CPLR 3103[a]). Here, for example, Supreme Court exempted from disclosure any photographs of plaintiff depicting nudity or romantic encounters.
Plaintiff suggests that disclosure of social media materials necessarily constitutes an unjustified invasion of privacy. We assume for purposes of resolving the narrow issue before us that some materials on a Facebook account may fairly be characterized as private. But even private materials may be subject to discovery if they are relevant. For example, medical records enjoy protection in many contexts under the physician-patient privilege (see CPLR 4504). But when a party commences an action, affirmatively placing a mental or physical condition in issue, certain privacy interests relating to relevant medical records – including the physician-patient privilege – are waived (see Arons v Jutkowitz, 9 NY3d 393, 409 [2007]; Dillenbeck v Hess, 73 NY2d 278, 287 [1989]). For purposes of disclosure, the threshold inquiry is not whether the materials sought are private but whether they are reasonably calculated to contain relevant information.

Applying these principles here, the Appellate Division erred in modifying Supreme Court’s order to further restrict disclosure of plaintiff’s Facebook account, limiting discovery to only those photographs plaintiff intended to introduce at trial. With respect

---

5 There is significant controversy on that question. Views range from the position taken by plaintiff that anything shielded by privacy settings is private, to the position taken by one commentator that “anything contained in a social media website is not ‘private’ . . . [S]ocial media exists to facilitate social behavior and is not intended to serve as a personal journal shielded from others or a database for storing thoughts and photos” (McPeak, The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery or Social Media Data, 48 Wake Forest L Rev 887, 929 [2013]).

6 Because plaintiff would be unlikely to offer at trial any photographs tending to contradict her claimed injuries or her version of the facts surrounding the accident, by limiting disclosure in this fashion the Appellate Division effectively denied disclosure of any evidence potentially relevant to the defense. To the extent the order may also contravene CPLR 3101(i), we note that neither party cited that provision in Supreme
to the items Supreme Court ordered to be disclosed (the only portion of the discovery request we may consider), defendant more than met his threshold burden of showing that plaintiff’s Facebook account was reasonably likely to yield relevant evidence. At her deposition, plaintiff indicated that, during the period prior to the accident, she posted “a lot” of photographs showing her active lifestyle. Likewise, given plaintiff’s acknowledged tendency to post photographs representative of her activities on Facebook, there was a basis to infer that photographs she posted after the accident might be reflective of her post-accident activities and/or limitations. The request for these photographs was reasonably calculated to yield evidence relevant to plaintiff’s assertion that she could no longer engage in the activities she enjoyed before the accident and that she had become reclusive. It happens in this case that the order was naturally limited in temporal scope because plaintiff deactivated her Facebook account six months after the accident and Supreme Court further exercised its discretion to exclude photographs showing nudity or romantic encounters, if any, presumably to avoid undue embarrassment or invasion of privacy.

In addition, it was reasonably likely that the data revealing the timing and number of characters in posted messages would be relevant to plaintiffs’ claim that she suffered cognitive injuries that caused her to have difficulty writing and using the computer, particularly her claim that she is painstakingly slow in crafting messages. Because Supreme Court provided defendant no access to the content of any messages on the Facebook account (an aspect of the order we cannot review given defendant’s failure to Court and we therefore have no occasion to further address its applicability, if any, to this dispute.
appeal to the Appellate Division), we have no occasion to further address whether defendant made a showing sufficient to obtain disclosure of such content and, if so, how the order could have been tailored, in light of the facts and circumstances of this case, to avoid discovery of nonrelevant materials.\(^7\)

In sum, the Appellate Division erred in concluding that defendant had not met his threshold burden of showing that the materials from plaintiff’s Facebook account that were ordered to be disclosed pursuant to Supreme Court’s order were reasonably calculated to contain evidence “material and necessary” to the litigation. A remittal is not necessary here because, in opposition to the motion, plaintiff neither made a claim of statutory privilege, nor offered any other specific reason – beyond the general assertion that defendant did not meet his threshold burden – why any of those materials should be shielded from disclosure.

Accordingly, the Appellate Division order insofar as appealed from should be reversed, with costs, the Supreme Court order reinstated and the certified question answered in the negative.

---

\(^7\) At oral argument, Supreme Court indicated that, depending on what the data ordered to be disclosed revealed concerning the frequency of plaintiff’s post-accident messages, defendant could possibly pursue a follow-up request for disclosure of the content. We express no views with respect to any such future application.
**Order insofar as appealed from reversed, with costs, order of Supreme Court, New York County, reinstated and certified question answered in the negative.** Opinion by Chief Judge DiFiore. Judges Rivera, Stein, Fahey, Garcia, Wilson and Feinman concur.

Decided February 13, 2018
The Sedona Conference Cooperation Proclamation

Dialogue Designed to Move the Law Forward in a Reasoned and Just Way
The Sedona Conference Cooperation Proclamation

Reprints
The Sedona Conference hereby expressly grants any interested party royalty-free reprint rights to this specific document.
The Sedona Conference Cooperation Proclamation

The Sedona Conference launches a coordinated effort to promote cooperation by all parties to the discovery process to achieve the goal of a “just, speedy, and inexpensive determination of every action.”

The costs associated with adversarial conduct in pre-trial discovery have become a serious burden to the American judicial system. This burden rises significantly in discovery of electronically stored information ("ESI"). In addition to rising monetary costs, courts have seen escalating motion practice, overreaching, obstruction, and extensive, but unproductive discovery disputes – in some cases precluding adjudication on the merits altogether – when parties treat the discovery process in an adversarial manner. Neither law nor logic compels these outcomes.

With this Proclamation, The Sedona Conference launches a national drive to promote open and forthright sharing of information by all parties to a case with the aim of expediting case progress, minimizing burden and expense, and removing contentiousness as much as practicable. If counsel fail in this combined duty to strive in the best interests of their clients to achieve the best results at a reasonable cost, with integrity and candor as officers of the court. Cooperation does not conflict with the advancement of their clients' interests - it enhances it. Only when lawyers confuse advocacy with adversarial conduct are these twin duties in conflict.

Lawyers preparing cases for trial need to focus on the full cost of their efforts – temporal, monetary, and human. Indeed, all stakeholders in the system – judges, lawyers, clients, and the general public – have an interest in establishing a culture of cooperation in the discovery process. Over-contentious discovery is a cost that has outstripped any advantage in the face of ESI and the data deluge. It is not in anyone's interest to waste resources on unnecessary disputes, and the legal system is strained by “gamesmanship” or “hiding the ball,” to no practical effect.

Effort to change the culture of discovery from adversarial conduct to cooperation is not utopian. It is, instead, an exercise in economy and logic. Establishing a culture of cooperation will channel valuable advocacy skills toward interpreting the facts and arguing the appropriate application of law.

---

1 Gartner RAS Core Research Note G00148170, Cost of eDiscovery Threatens to Skew Justice System, 1D# G00148170, (April 20, 2007), at http://www.h5technologies.com/pdf/gartner0607.pdf. (While noting that “several . . . disagreed with the suggestion [to collaborate in the discovery process] . . . calling it ‘utopian’, one of the “take-away[s]” from the program identified in the Gartner Report was to “[s]trive for a collaborative environment when it comes to eDiscovery, seeking to cooperate with adversaries as effectively as possible to share the value and reduce costs.”).
The Sedona Conference Cooperation Proclamation

Cooperative Discovery is Required by the Rules of Civil Procedure

When the first uniform civil procedure rules allowing discovery were adopted in the late 1930s, “discovery” was understood as an essentially cooperative, rule-based, party-driven process, designed to exchange relevant information. The goal was to avoid gamesmanship and surprise at trial. Over time, discovery has evolved into a complicated, lengthy procedure requiring tremendous expenditures of client funds, along with legal and judicial resources. These costs often overshadow efforts to resolve the matter itself. The 2006 amendments to the Federal Rules specifically focused on discovery of “electronically stored information” and emphasized early communication and cooperation in an effort to streamline information exchange, and avoid costly unproductive disputes.

Discovery rules frequently compel parties to meet and confer regarding data preservation, form of production, and assertions of privilege. Beyond this, parties wishing to litigate discovery disputes must certify their efforts to resolve their difficulties in good faith.

Courts see these rules as a mandate for counsel to act cooperatively. Methods to accomplish this cooperation may include:

1. Utilizing internal ESI discovery “point persons” to assist counsel in preparing requests and responses;
2. Exchanging information on relevant data sources, including those not being searched, or scheduling early disclosures on the topic of Electronically Stored Information;
3. Jointly developing automated search and retrieval methodologies to cull relevant information;
4. Promoting early identification of form or forms of production;
5. Developing case-long discovery budgets based on proportionality principles; and
6. Considering court-appointed experts, volunteer mediators, or formal ADR programs to resolve discovery disputes.

The Road to Cooperation

It is unrealistic to expect a *sua sponte* outbreak of pre-trial discovery cooperation. Lawyers frequently treat discovery conferences as perfunctory obligations. They may fail to recognize or act on opportunities to make discovery easier, less costly, and more productive. New lawyers may not yet have developed cooperative advocacy skills, and senior lawyers may cling to a long-held “hide the ball” mentality. Lawyers who recognize the value of resources such as ADR and special masters may nevertheless overlook their application to discovery. And, there remain obstreperous counsel with no interest in cooperation, leaving even the best-intentioned to wonder if “playing fair” is worth it.

2 See, e.g., *Board of Regents of University of Nebraska v BASF Corp.* No. 4:04-CV-3356, 2007 WL 3342423, at *5 (D. Neb. Nov. 5, 2007) (“The overriding theme of recent amendments to the discovery rules has been open and forthright sharing of information by all parties to a case with the aim of expediting case progress, minimizing burden and expense, and removing contentiousness as much as practicable. [citations omitted]. If counsel fail in this responsibility—willfully or not—their principles of an open discovery process are undermined, coextensively inhibiting the courts’ ability to objectively resolve their clients’ disputes and the credibility of its resolution.”).
The Sedona Conference Cooperation Proclamation

This “Cooperation Proclamation” calls for a paradigm shift for the discovery process; success will not be instant. The Sedona Conference views this as a three-part process to be undertaken by The Sedona Conference Working Group on Electronic Document Retention and Production (WG1):

Part I: Awareness - Promoting awareness of the need and advantages of cooperation, coupled with a call to action. This process has been initiated by The Sedona Conference Cooperation Proclamation.

Part II: Commitment - Developing a detailed understanding and full articulation of the issues and changes needed to obtain cooperative fact-finding. This will take the form of a “Case for Cooperation” which will reflect viewpoints of all legal system stakeholders. It will incorporate disciplines outside the law, aiming to understand the separate and sometimes conflicting interests and motivations of judges, mediators and arbitrators, plaintiff and defense counsel, individual and corporate clients, technical consultants and litigation support providers, and the public at large.

Part III: Tools - Developing and distributing practical “toolkits” to train and support lawyers, judges, other professionals, and students in techniques of discovery cooperation, collaboration, and transparency. Components will include training programs tailored to each stakeholder; a clearinghouse of practical resources, including form agreements, case management orders, discovery protocols, etc.; court-annexed e-discovery ADR with qualified counselors and mediators, available to assist parties of limited means; guides for judges faced with motions for sanctions; law school programs to train students in the technical, legal, and cooperative aspects of e-discovery; and programs to assist individuals and businesses with basic e-record management, in an effort to avoid discovery problems altogether.

Conclusion

It is time to build upon modern Rules amendments, state and federal, which address e-discovery. Using this springboard, the legal profession can engage in a comprehensive effort to promote pre-trial discovery cooperation. Our “officer of the court” duties demand no less. This project is not utopian; rather, it is a tailored effort to effectuate the mandate of court rules calling for a “just, speedy, and inexpensive determination of every action” and the fundamental ethical principles governing our profession.
Appendix
<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Position</th>
<th>Term Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member 2019</td>
<td>Carol V. Clark</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2019</td>
<td>Harold T. Daniel, Jr.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Laverne Lewis Gaskins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Allegra J. Lawrence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>C. James McCallar, Jr.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Jennifer Campbell Mock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Patrick T. O'Connor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Kenneth L. Shigley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>A. James Elliott</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Buddy M. Mears</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Dean Daisy Hurst Floyd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Carol Ellis Morgan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Hon. Harold David Melton</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Jeffrey Reese Davis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member 2018</td>
<td>Tangela Sarita King</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Appendix**

- Emory University
- John Marshall
- Mercer University
- University of Georgia
- Liaison
- Staff Liaison 2018
- Cassady Vaughn Brewer
- Member 2019
## ICLE BOARD

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Term Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cassady Vaughn Brewer</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>Carol V. Clark</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>Harold T. Daniel, Jr.</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>Laverne Lewis Gaskins</td>
<td>Member</td>
<td>2018</td>
</tr>
<tr>
<td>Allegra J. Lawrence</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>C. James McCallar, Jr.</td>
<td>Member</td>
<td>2018</td>
</tr>
<tr>
<td>Jennifer Campbell Mock</td>
<td>Member</td>
<td>2020</td>
</tr>
<tr>
<td>Patrick T. O'Connor</td>
<td>Member</td>
<td>2018</td>
</tr>
<tr>
<td>Kenneth L. Shigley</td>
<td>Member</td>
<td>2020</td>
</tr>
<tr>
<td>A. James Elliott</td>
<td>Emory University</td>
<td>2019</td>
</tr>
<tr>
<td>Buddy M. Mears</td>
<td>John Marshall</td>
<td>2019</td>
</tr>
<tr>
<td>Dean Daisy Hurst Floyd</td>
<td>Mercer University</td>
<td>2019</td>
</tr>
<tr>
<td>Carol Ellis Morgan</td>
<td>University of Georgia</td>
<td>2019</td>
</tr>
<tr>
<td>Hon. Harold David Melton</td>
<td>Liaison</td>
<td>2018</td>
</tr>
<tr>
<td>Jeffrey Reese Davis</td>
<td>Staff Liaison</td>
<td>2018</td>
</tr>
<tr>
<td>Tangela Sarita King</td>
<td>Staff Liaison</td>
<td>2018</td>
</tr>
</tbody>
</table>
GEORGIA MANDATORY CLE FACT SHEET

Every “active” attorney in Georgia must attend 12 “approved” CLE hours of instruction annually, with one of the CLE hours being in the area of legal ethics and one of the CLE hours being in the area of professionalism. Furthermore, any attorney who appears as sole or lead counsel in the Superior or State Courts of Georgia in any contested civil case or in the trial of a criminal case in 1990 or in any subsequent calendar year, must complete for such year a minimum of three hours of continuing legal education activity in the area of trial practice. These trial practice hours are included in, and not in addition to, the 12 hour requirement. ICLE is an “accredited” provider of “approved” CLE instruction.

Excess creditable CLE hours (i.e., over 12) earned in one CY may be carried over into the next succeeding CY. Excess ethics and professionalism credits may be carried over for two years. Excess trial practice hours may be carried over for one year.

A portion of your ICLE name tag is your ATTENDANCE CONFIRMATION which indicates the program name, date, amount paid, CLE hours (including ethics, professionalism and trial practice, if any) and should be retained for your personal CLE and tax records. DO NOT SEND THIS CARD TO THE COMMISSION!

ICLE will electronically transmit computerized CLE attendance records directly into the Official State Bar Membership computer records for recording on the attendee’s Bar record. Attendees at ICLE programs need do nothing more as their attendance will be recorded in their Bar record.

Should you need CLE credit in a state other than Georgia, please inquire as to the procedure at the registration desk. ICLE does not guarantee credit in any state other than Georgia.

If you have any questions concerning attendance credit at ICLE seminars, please call: 678-529-6688
Follow ICLE on social media:

http://www.facebook.com/iclega

bit.ly/ICLELinkedIn

#iclega
#TuesAt2