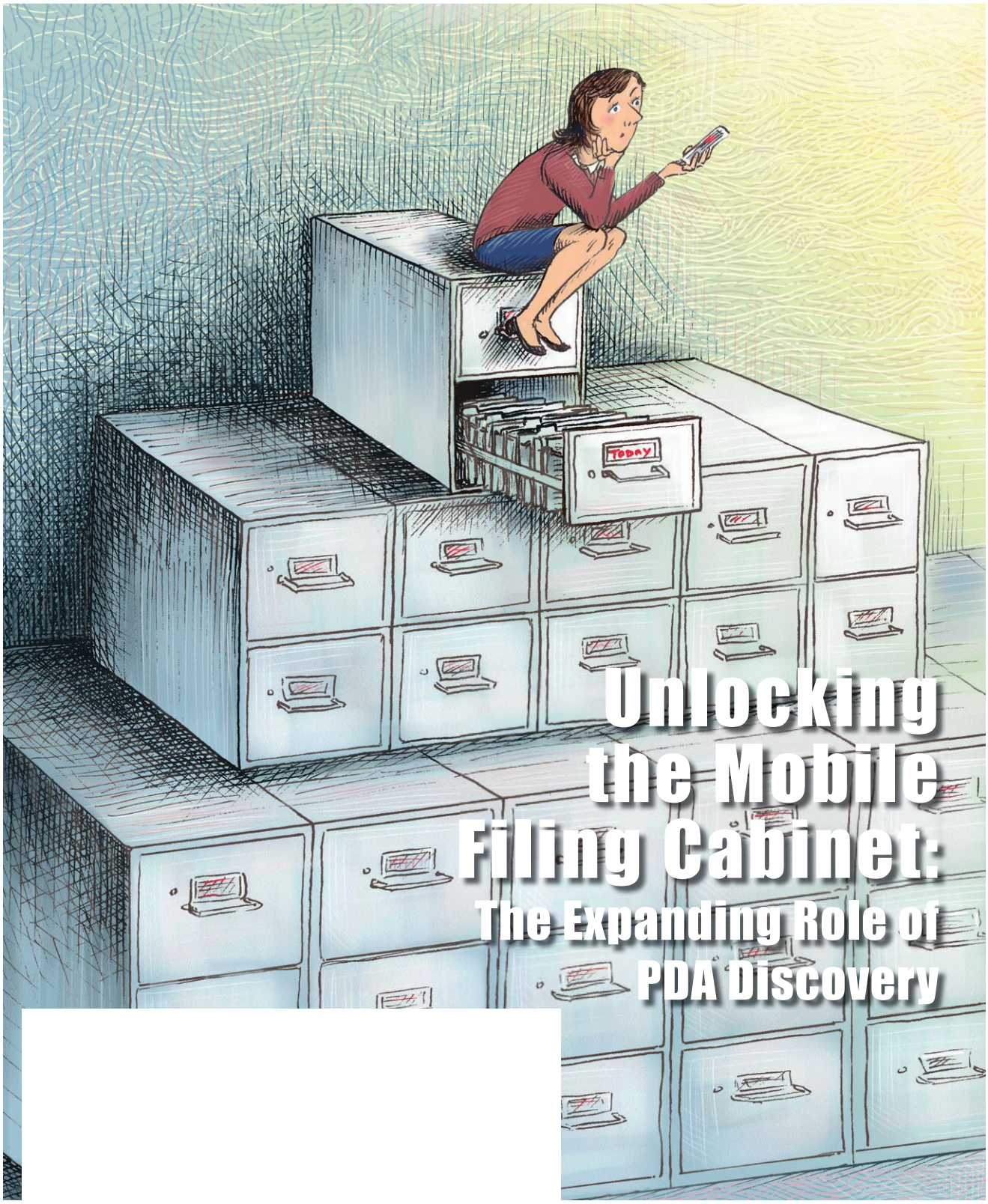
THE FLORIDA
VOLUME 90, NO. 10 DECEMBER 2016

BAR JOURNAL

ADVANCING THE COMPETENCE AND PUBLIC RESPONSIBILITY OF LAWYERS



Unlocking the Mobile Filing Cabinet:

The Expanding Role of PDA Discovery

contents

THE FLORIDA
BAR JOURNAL

651 East Jefferson Street
Tallahassee, Florida 32399-2300
(850) 561-5600
FloridaBar.org

Court-related information, flcourts.org

Publisher
John F. Harkness, Jr.

Editor
Cheryle M. Dodd

Associate Editor
Melinda Melendez

Associate Editor
Rawan Bitar

Advertising
Randy Traynor

Circulation/Administration
Cheryl Morgan

Published monthly except July/August and September/October, which are combined issues, by The Florida Bar, 651 East Jefferson Street, Tallahassee 32399-2300, telephone (850) 561-5600. Periodicals postage paid at the Post Office in Tallahassee, Florida 32399-2300 and at additional mailing offices. The Florida Bar *Journal*, ISSN 0015-3915, Pub. No. 200-960.

Subscriptions: Florida Bar members receive the *Journal* as part of their annual fee payment. Nonmember subscriptions are $50 a year; single magazine copies, $5. Single copy sales subject to Florida sales tax.

The *Journal* will accept all advertising that otherwise is in keeping with the publication's standards of ethics, legality, and propriety, so long as such advertising is not derogatory or demeaning. Advertising is not accepted by which the advertiser violates or enables another to violate the Rules of Professional Conduct or the Florida Code of Judicial Conduct. The opinions and interpretations of staff counsel and appropriate committees of The Florida Bar charged with authority to interpret the codes will be controlling. Advertising copy is reviewed, but publication herein does not imply endorsement of any product, service or opinion advertised.

Views and conclusions expressed in articles herein are those of the authors and not necessarily those of the editorial staff, officials, or Board of Governors of The Florida Bar.

The Florida Bar *Journal* welcomes letters to the editor. Letters should be no longer than 500 words. Letters should focus comments or criticism on issues, rather than individuals acting in their individual capacities, and should not be defamatory. Comments also may be clarified or edited by staff as required based on space considerations and the number and nature of comments received on any single topic. Letters are considered property of the *Journal*, and also may be displayed electronically on The Florida Bar's website and made available commercially through affinity partners of the Bar. Letters should be directed to "Letters to the Editor," The Florida Bar *Journal*, 651 E. Jefferson St., Tallahassee, FL 32399-2300 or emailed to cdodd@floridabar.org.

POSTMASTER: Send change of address to The Florida Bar, Membership Records, 651 E. Jefferson St., Tallahassee, FL 32399-2300.

Features

Columns

Cover by Barbara Kelley

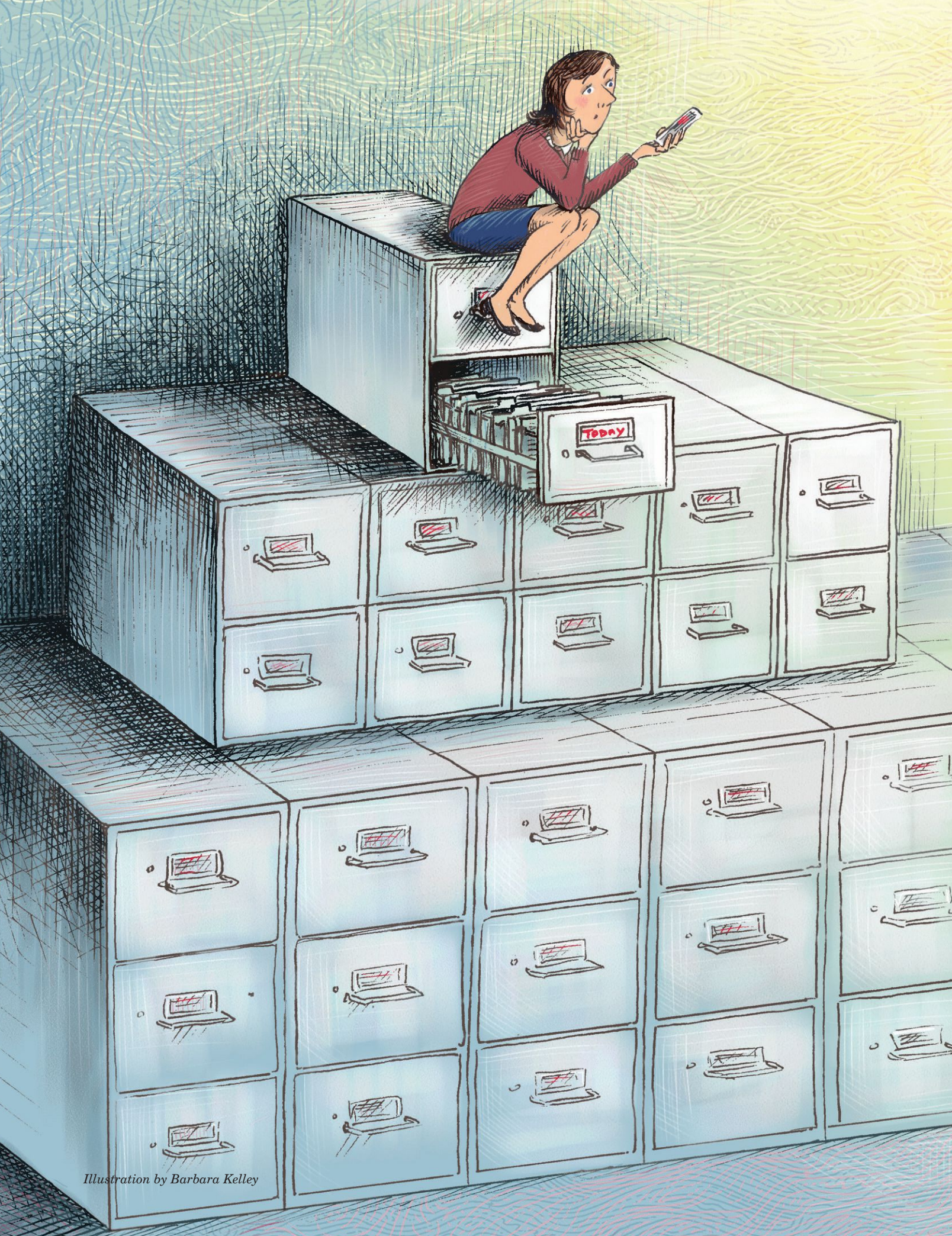


Illustration by Barbara Kelley

Unlocking the Mobile Filing Cabinet: The Expanding Role of PDA Discovery

by Michael R. Holt

The letters "PDA" are no longer synonymous with "public displays of affection." These days, "personal data assistants" are all the rage. In just a short time, PDAs revolutionized the way we live and communicate. They are now a prominent part of our everyday lives. Devices like smartphones, tablets, "phablets," and even watches enable us to send, share, or receive seemingly limitless amounts of data.

Along with these devices come "apps" — *millions* of them.[1] As the Supreme Court recently observed, "the phrase 'there's an app for that' is now part of the popular lexicon."[2] Among other things, they help us take notes, manage our schedules, stay in touch with friends and business contacts, find significant others, watch movies, play games, shop, pay our bills, and count calories. Viewed collectively, these apps "form a revealing montage of the user's life."[3]

Just how helpful is all of this technology? Does it make the world better, worse, or somewhere in between? This is the subject of fascinating debate well beyond the scope of this article. What cannot be ignored is that people from all walks of life are glued to their PDAs. Need a reminder? Visit any restaurant, movie, sporting event,[4] or even a gym to observe the "smartphone slump" in action.[5]

This constant activity generates colossal amounts of discoverable information beyond emails and texts. The device itself can reveal a snapshot or portrait of someone's life and ultimately, their ability to function. Indeed,"[c]ultural boundaries between the personal and professional blend as round-the-clock email, texting, and networking sites became first socially acceptable, then the work place standard."[6] As the social network explodes, PDA content becomes an ever more prominent part of litigation. Two recent high-profile matters involve deflated footballs and a senseless act of terrorism.[7]

Sometimes, the *use* of a PDA is just as important as what is *on* it. For example, consider a claimant seeking damages based on reduced cognitive functioning. The claimant's PDA interaction could very well reveal information to refute the claim or otherwise corroborate it. Lawyers in careless driving cases may want to discover PDA activity beyond simple texting to demonstrate inattention to the road. And employment lawyers may have a keen interest in how their opponents interact with their PDAs while at work. The list goes on.

A discovery request seeking this type of electronic information reflects today's changing society and its ever-increasing reliance on cellular devices as a means of communication, information, and entertainment. Even the most rudimentary cellular devices contain a litany of different applications, games, programs, and other modes of communication, which directly relate to underlying litigation issues.

This raises the question of whether counsel may access, inspect, and mine information from the device itself. Traditionally, Florida's courts deny unfettered access to electronic information without some showing that the opponent hid information or otherwise failed to cooperate. That is not always the case with a PDA, where the focus of the request and analysis are different.

This article explores the phenomena of PDAs, when their examination might be appropriate and how to open the digital "filing cabinet." Also discussed are the use of experts to assist with examination and data extraction.

Caselaw concerning electronic discovery traces its origin back to computer hard drives, not PDAs. Over time though, Florida's appellate courts applied this law to evolving technology, including mobile devices.While courts once restricted electronic discovery to cases involving discovery noncompliance, the door is now guardedly opening in certain circumstances.

Ultimately, PDA discovery in the appropriate case can dramatically impact the strength of both claims and defenses.

PDAs and Their Increasingly Prominent Societal Role

PDAs are loaded with potentially relevant information. A recent U.S. Supreme Court opinion thoroughly discusses this, albeit in a different context. That decision, *Riley v. California,* 134 S. Ct. 2473 (2014), recognized and elaborated upon the prominent roles that PDAs now play in our daily lives.

The underlying case concerned whether police may search the cell phone contents of an arrestee without getting a warrant (the court said "no").[8] Discussing this issue, the Court humorously observed that modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they are an important feature of human anatomy."[9]

The Court also marveled at the storage capabilities of a cell phone compared to an old-fashioned wallet. "Cell phones…place vast quantities of personal information literally in the hands of individuals."[10] These devices are "minicomputers" with an "immense storage capacity."[11] Cell phones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[12] They "also happen to have the capacity to be used as a telephone."[13]

These devices not only store information, they leave behind a trail that provides insight (sometimes not welcome) into the lives of users. "An internet search and browsing history, for example, can be found on an internet-enabled phone and could reveal an individual's private interest or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[14] Indeed, "[h]istoric location information is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but within a particular building."[15]

Summing up, PDAs "reveal much more in combination than any isolated record."[16] Additionally, the capacity of cell phones ensure that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[17] The data on that phone "can date back to the purchase of the phone, or even earlier."[18] "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[19]

These words powerfully illustrate the vast amount of available information and the reasons and why that data might be relevant to legal proceedings.[20] But can attorneys *begin* the discovery process by immediately requesting access to the device(s) themselves, as opposed the information they store? Not so fast. As Florida's caselaw makes clear, there is no "one size fits all" when it comes to PDA discovery. Given the right factual circumstances, planning, and carefully tailored requests, PDA inspections are certainly available and should be pursued.

Florida's Existing Legal Framework for Device Discovery

There are no specific rules, laws, or statutes solely focused upon PDA discovery. The process starts with a request for production or inspection under the applicable rules of procedure. A responding party may well object on the grounds that discovery cannot *start* with the forensic examination of a mobile device.

Caselaw concerning electronic discovery traces its origin back to computer hard drives, not PDAs. Over time though, Florida's appellate courts applied this law to evolving technology, including mobile devices. While courts once restricted electronic discovery to cases involving discovery noncompliance, the door is now guardedly opening in certain circumstances. The three cases discussed below, *Menke v. Broward County School Board*, 916 So. 2d 8 (Fla. 4th DCA 2005); *Holland v. Barfield,* 35 So. 3d 953 (Fla. 5th DCA 2010); and *Antico v. Sindt Trucking, Inc.*, 148 So. 3d 163 (Fla. 1st DCA 2014), illustrate this evolution.

Menke v. Broward County School Board

In *Menke,* the Fourth District Court of Appeal quashed an ALJ's order compelling production of all computers in a teacher's home. That case involved a disciplinary proceeding against a high-school teacher accused of inappropriately communicating with students. The

The court very accurately analogized a computer to an "electronic filing cabinet" from which parties may extract information, including the time spent on internet sites or chat rooms. Unfettered forensic inspections are, by their very nature, invasive and often, overly thorough. The wholesale access allowed by the ALJ, with only limited safeguards, would "expose confidential communications and matters entirely extraneous...."

school board, in seeking his termination, requested a broad forensic inspection.

The court very accurately analogized a computer to an "electronic filing cabinet" from which parties may extract information, including the time spent on internet sites or chat rooms.[21] Unfettered forensic inspections are, by their very nature, invasive and often, overly thorough. The wholesale access allowed by the ALJ, with only limited safeguards, would "expose confidential communications and matters entirely extraneous to the present litigation, such as banking records."[22]

Rule 1.350(a)(3), the court observed, was "broad enough to encompass requests to examine a computer hard drive but only in limited and strictly controlled circumstances… unlimited access to anything on the computer would constitute irreparable harm, because it would expose confidential, privileged information to the opposing party."[23] *If* the opponent demonstrated that the adversary deleted information, a computer search "might be appropriate."[24]

Against this background, "intrusive searching of the entire computer by an opposing party should not be the first means of obtaining the relevant information."[25] Because there was "no evidence of any destruction of evidence or thwarting of discovery" and because the search allowed access to "literally everything on the petitioner's computers," the ALJ's order caused irreparable harm. The court did not completely foreclose the possibility of such discovery. Instead, a forensic search *might* be appropriate if the requesting party proved 1) evidence of any destruction of evidence or thwarting of discovery; 2) a likelihood the information exists on the devices; and 3) no less intrusive means exists of obtaining the information.[26]

Holland v. Barfield

Several years later, the Fifth District Court of Appeal granted a certiorari petition, quashing an order compelling production of the defendant's computer hard drive and cell phone. The underlying case was a wrongful death action. The plaintiff served discovery seeking production of "[a]ny and all computer hard drives" and "all cell phones" possessed by the defendant from the day before the accident to the present.[27]

The defendant, a college student, argued the requests were overbroad, involved impermissible "fishing" and invaded her privacy.[28] The plaintiff sought these devices to discover "evidence of communications among the defendants through mobile phone text messages, Facebook.com, and MySpace.com."[29]

The defendant sought certiorari from an order compelling production. She advanced several arguments, among them that the order allowed the plaintiff to review information outside the presence of her counsel, that she should have an opportunity to review information before handing over the devices and that being without them would hinder her preparation for class and communication with students and faculty.[30]

The Fifth DCA noted, like *Menke*, the record contained no evidence of "destruction of evidence or thwarting of discovery."[31] And the production request sought "the electronic media themselves" rather than "specific information contained therein."[32] Additionally, the sought-after discovery was already available through less intrusive means.[33] The order would, the court found, allow the plaintiff to "review, without limit or time frame, all of the information contained in [p]etitioner's computer and mobile phone SIM card without regard to her constitutional right of privacy and the right against self-incrimination privileges, including attorney-client, work product."[34] This, the court concluded, "caused irreparable harm."[35]

Antico v. Sindt Trucking, Inc.

In 2014, the First District Court of Appeal confronted a wrongful death claim brought on behalf of a driver killed in a collision with a truck. The defendant trucking company sought and obtained an order allowing its expert to inspect data from the driver's mobile phone on the day of the accident.

While *Menke* and *Holland* might support granting the plaintiff's petition, the appellate court denied it. In so doing, *Antico* carefully examined the circumstances regarding the underlying claim in conjunction with the parameters of the request.

The decedent was allegedly "distracted by her iPhone" before the accident.[36] The defendants initially sought and obtained some data from the cellphone (calling and texting records). But other data, "such as use

and location information, internet website access history, email messages, and social and photo media posted and reviewed on the day of the accident," was not produced.[37] The plaintiff resisted the request for a device inspection based on a violation of the decedent's privacy rights under the Florida Constitution.[38]

The order granting inspection recognized these interests. It also emphasized that two witnesses reported the decedent may have been using her cell phone at the time of the accident.[39] The order "set strict parameters" governing the inspection.[40] This included videotaping the inspection, installing software to guard against alteration of the phone's hard drive, making a master copy for review by the plaintiff's counsel and limiting the time period available for review.[41]

Cases like *Menke* and *Holland,* the court found, did not completely preclude electronic device discovery.[42] The "context" of the discovery request was important, as it did not "involve an unanchored fishing expedition."[43] Instead, the defendant predicated the request upon "specific evidence" suggesting that the decedent may have been "texting just before the accident."[44]

The multi-faceted nature of cellular phones and their many uses also apparently influenced the court's holding. Indeed, "the only way to discover whether the decedent used her cellphone's integrated software at the time of the accident, or drafted a text, dialed a number, searched for contact information, reviewed an old message, or used any other of the smartphone's many features, is by broadly inspecting data associated with all of the cell phone's applications."[45]

The trial court's order protected the decedent's privacy interests through a strict protocol.[46] And, because the plaintiff "offered nothing in response to the court's privacy concerns and open invitation to propose a different process," the court could not "conclude that the trial court erred by allowing [r]espondents' expert retrieve the cellphone's data under limited and controlled conditions."[47]

Ultimately, if the goal is to measure *use* of the device, it may seem very difficult to *start* anywhere else. Ultimately, PDA discovery involves a weighing and balancing which turns upon the nature of the claim, the parameters of the inspection, and the protections available to the opponent.

Opening the File Cabinet: Nuts and Bolts of PDA Discovery

Without question, cellular phone data and social media are discoverable when the content relates to the salient issues.[48] With respect to social media, instant messaging, and similar applications — such material is not absolutely privileged or protected solely by the right to privacy.[49] In certain instances, documenting PDA usage *in totality* may ultimately help demonstrate the quality of a person's life and whether either they are an "accurate reporter of his/her [post-accident] life or the quality of her life since then."[50] As

Antico teaches, parties may obtain PDA discovery where the inspection is limited and controlled.[51]

Lawyers seeking production of mobile devices must start the discovery process with a well thought-out plan. Although *Menke, Holland*, and *Antico* do not explicitly require discovery to proceed in stages, prudent counsel will nevertheless employ it. Doing so will enable the parties and, if necessary, the court, to focus the issues as to any physical inspection.

Once litigation becomes imminent, preservation letters should reference not only information within the PDAs but the devices themselves. After the lawsuit filing, discovery requests can pinpoint the number and type of available devices along with information regarding their use. This includes mobile messaging apps like Snapchat, WhatsApp, Kik Messenger, Skype, Tinder, and Yikyak.[52]

Counsel may, during this process, obtain hard copies of printable content. This can provide valuable assistance when developing a device inspection protocol. It can also help determine whether the targeted extraction should include any data deleted from the PDA's memory system.

As with all discovery, requests should be broad enough to obtain the sought-after information but not so expansive to draw a valid objection. Thinking through the issues and limiting the scope of the proposed data extraction ultimately saves valuable time, money, and judicial resources. Requests should limit themselves to data, communications, or application usage that relate to the lawsuit, sought-after damages, or defenses.[53]

A Word About Forensic Examinations

The technical nature of PDA discovery and the need to ensure privacy and security highlight the need for lawyers to seek help from forensic examiners. Counsel should not approach civil litigation "as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail…."[54] Rather, collection methods must be reasonable and appropriate for the circumstances of the case.[55]

Cell phone forensic experts specialize in retrieval of mobile data and preservation of evidence to ensure its admissibility in court. However, these forensic experts come at a price the client must be willing to pay.[56]

Forensic experts employ a variety of data collection methods. These vary based upon the specific needs of a case. For example, an expert may make a "forensic logical copy," which collects pictures, text messages, and emails.[57] A forensic image, on the other hand, is a "copy of *all data* on a device in manner that represents the entire state of the device and could clone an exact duplicate with equivalent hardware." This type of forensic examination does not collect unsaved data from volatile memory.[58]

Another method involves the "logical collection of synchronized data."[59] This collects information from a location synced with the device itself.[60] Synchronized data locations such as, Facebook, Gmail, DropBox, and iCloud, can be accessed from more than one device such as an app on a cell phone or webpage on a computer.[61] Because of that, the data may not be in one central location.[62]

Cloud storage is another service. "These services are completely hosted by third-party companies each of which have processes that must be followed if anyone other than the user or the paired device wants to collect the hosted backups."[63] The premise behind cloud storage is that data can be accessed from anywhere all the time.[64]

Similar to cloud storage is file sharing or a "company-owned and managed server or share and likely only used for select applications such as [Microsoft] Exchange, for centralized management of company owned devices."[65] However, some data may not be available from this server, such as anything saved locally to the computer as opposed to the file sharing site or application.[66]

Conclusion

PDA discovery has its place in Florida's litigation landscape. Lawyers must carefully tailor their requests in light of the facts and alleged damages. Overly broad requests allow access to irrelevant information, thus, intruding on the privacy aspects carefully examined by the Supreme Court in *Riley*. Requesting parties should enlist appropriately qualified personnel to handle any data distraction with minimal interruption and without altering or damaging the device. Litigants receiving overly broad requests still, of course, retain all the protections of the Florida Rules of Civil Procedure. They should also strongly consider enlisting the assistance of third-party experts who can assist opposing counsel, as well as the trial court, with the technical aspects concerning any objections.❑

[1] Even the great Don Rickles has an app called "Mr. Warmth," which "turns your iPhone into a Las Vegas Showroom." Don Rickles, Don Rickles Mr. Warmth App, http://mrwarmth.donrickles.com/.

[2] *Riley v. California,* ___ U.S. ___, 134 S. Ct. 2473, 2490 189 L .Ed. 2d 430 (2014).

[3] *Id.* at 2490.

[4] Melissa Chan, *Selfie-taking Sorority Girls Get Shamed at a Diamondbacks Game*, NY Daily News (Oct. 1, 2015), *available at* http://www.nydailynews.com/sports/baseball/selfie-taking-sorority-girls-shamed-diamondback-game-article-1.2381798.

[5] Not only does the tilting of one's head cause users to "look like Lurch," it can lead to physical problems as well. *See* Jessica Firger, *OMG, You're Texting Your Way to Back Pain,* CBS News (Nov. 14, 2014), http://www.cbsnews.com/news/omg-youre-texting-your-way-to-back-pain/; *see also* Maryann Berry, Cell Phone Ergonomics: How to Avoid the "Smart Phone Slump," http://breakingmuscle.com/mobility-recovery/cell-phone-ergonomics-how-to-avoid-the-smart-phone-slump.

[6] Kate Paslin, *Mobile Devices as Discoverable Data,* American Bar Association (Feb. 12, 2013), http://apps.americanbar.org/litigation/committees/technology/articles/winter2013-0213-mobile-devices-as-discoverable-data.html. Justice Rosenbaum, concurring in a criminal case involving a Fourth Amendment issue, aptly remarked that "[i]n our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life." *United States v. Davis*, 785 F.3d 498, 525 (11th Cir. 2015), *cert. den.*, 136 S. Ct. 479, 193 L. Ed. 2d 349 (2015).

[7] *National Football League Management Council v. National Football League Players Association,* Case Nos. 15 Civ. 5916

(RMB)(JCF) and 5982 (RMB)(JCF) (S.D. N.Y. Sept. 3, 2015); Apple, A Message to Our Customers, http://www.apple.com/customer-letter/ (Apple C.E.O. Tim Cook explained the company's use of "encryption to protect our customers' personal data….").

[8] *Riley,* 134 S. Ct. at 2494.

[9] *Id*. at 2484

[10] *Id*. at 2485.

[11] *Id*. at 2489.

[12] *Id*.

[13] *Id*.

[14] *Id.*

[15] *Id*. at 2490.

[16] *Id.* at 2479.

[17] *Id.* at 2489.

[18] *Id*.

[19] *Id.* (Citation omitted).

[20] Not only does this data reside on the PDA itself, but also in the hands of third-party service providers. This includes "the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the email addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers." *U.S. v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor J., concurring) (quoting Alito J., concurring at 962). These represent additional potential sources of discovery practitioners should consider.

[21] *Menke v. Broward Cnty School Board*, 916 So. 2d 8, 10 (Fla. 4th DCA 2005).

[22] *Id.*

[23] *Id*. at 11 (citation omitted).

[24] *Id.*

[25] *Id.* at 11-12.

[26] *Id.* at 12.

[27] *Holland v. Barfield*, 35 So. 3d 953, 954 (Fla. 5th DCA 2010).

[28] *Id.*

[29] *Id.*

[30] *Id*.

[31] *Id.* at 955.

[32] *Id*. at 955-56.

[33] *Id*.

[34] *Id.*

[35] *Id*. at 956.

[36] *Antico v. Sindt Trucking Inc.*, 148 So. 3d 163, 164 (Fla. 1st DCA 2014).

[37] *Id.* at 165.

[38] *Id*.

[39] *Id*. at 164-165.

[40] *Id*. at 165.

[41] *Id*.

[42] *Id*.

[43] *Id*. at 166.

[44] *Id.* at 166-67.

[45] *Id*. at 168.

[46] *Id.*

[47] *Id*. at 167-68. Several Florida federal court decisions also touch upon these issues. *See Carolina Bedding Direct, LLC v. Downen*, No. 3:13-cv-336-J-32MCR, 2013 WL 1899743 at *2 (M.D. Fla. May 7, 2013) (denying emergency motion to compel inspection of computer hard drives or electronic devices used by defendant in non-compete/non-solicitation case where plaintiff did not show that defendant engaged in improper conduct or that it could not obtain documents through "specific production requests"); *Wynmoor Community Council, Inc. v. QBE Ins. Co.*, 280 F.R.D. 681, 687 (S.D. Fla. 2012) (granting defendant's motion to compel forensic examination of computer hard drive and establishing a "collection and review" protocol where plaintiff had "not made any effort to retrieve ESI in response to Defendant's discovery requests"); *Bank of Mongolia v. M&P Global Financial Services, Inc.*, 258 F.R.D. 514, 520-521 (S.D. Fla. 2009) (granting motion to compel forensic computer inspection when plaintiff obtained information from third parties, "which appear to be records that the…defendants should have had"); *U&I Cor. V. Advanced Medical Design, Inc*., 251 F.R.D. 667, 676 (M.D. Fla. 2008) (granting distributor limited inspection of manufacturer's computer hard drives in breach of contract action where distributor made sufficient factual showing of noncompliance with discovery; "It is not the court's role, nor that of opposing counsel, to drag a party kicking and screaming through the discovery process."). *See also MCPA King of Spades v. T.E.C. Broadcasting Inc.*, Civil Action No. 1:11cv00080, 2012 WL 1203372 at *2 (W.D. Va. April 10, 2012) (allowing forensic inspection of defendant radio station's computers to access playlists in copyright infringement action: "[T]he need to recover this information has been necessitated by the defendants' purposeful failure to retain these logs in an easily accessible format, a failure that continued after the filing of this litigation and after specific discovery requests for the information being routinely discarded.").

[48] *See Nucci v. Target Corp.*, 162 So. 3d 146, 152-54 (Fla. 4th DCA 2015).

[49] *Id.* at 152-54.

[50] *Id.* at 152.

[51] *Id.* (rejecting arguments of a so-called "fishing expedition" where the party seeking the discovery provided limited and controlled parameters). Decisions from other judicial districts highlight the importance of narrowly tailored requests. *Compare Freres v. Xyngular Corp.*, No. 2:13–cv–400–DAK–PMW, 2014 WL 1320273 at *4-5 (D. Utah March 31, 2014) (granting motion to compel inspection and copying of plaintiff's cell phone in wrongful termination case where the defendant proposed "a very specific process for conducting the copying and inspection, as well as the narrow category of information it seeks") *with Bakhit v. Safety Marketing, Inc.*, Civ. No. 3:13CV1049, 2014 WL 2916490 at *2-3 (D. Conn. June 26, 2014) (in race discrimination case, denying plaintiff's request, without prejudice, to inspect cell phones of 10 of the defendant's employees when defendant's foreman allegedly shared racist texts and jokes; request was too overly broad and intrusive, and plaintiffs did not demonstrate an inability to obtain the information through other means).

[52] Sara Anne Hook & Cori Faklaris, *Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik and Other Mobile Messaging Apps*, The Federal Lawyer at 67-68 (May 2016). This article provides an excellent discussion of these and other apps and issues associated with extracting information from them.

[53] Such requests are also subject to the proportionality limitations applicable to all discovery. *See* FRCP 26(b)(2)(C). This includes the prohibition of discovery that is "unreasonably cumulative or duplicative, or that could be obtained from some more convenient, less burdensome or less expensive source, or the benefit of which is outweighed by its burden or expense, when considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake and the importance of the proposed discovery to those issues." *Nola Spice Designs, LLC v. Haydel Enters.,* No. 12-2515, 2013 WL 3974535 at *2 (E.D. La. Aug. 2, 2013).

[54] *John B. v. Goetz*, 531 F.3d 448, 460 (6th Cir. 2008) (quoting *McCurdy Group, LLC v. Am. Biomedical Group, Inc*., 9 Fed. Appx. 822, 831 (10th Cir. 2001)).

[55] Michael Arnold & Dennis R. Kiker, *The Big Data Collection Problem of Little Mobile Devices,* Rich. J. L. & Tech. (Mar. 25, 2015), *available at* http://jolt.richmond.edu/index.php/the-big-data-collection-problem-of-little-mobile-devices/.

[56] Depending on the quantity of data and type of device, a forensic expert may cost around $800 or more if the amount of devices increase, such as through an office or company. *See* Kate Paslin, *Mobile Devices as Discoverable Data,* American Bar Association (Feb. 12, 2013), *available at* http://apps.americanbar.org/litigation/committees/technology/articles/winter2013-0213-mobile-devices-as-discoverable-data.html.

[57] *See* Arnold & Kiker*, The Big Data Collection Problem of Little Mobile Devices,* Rich. J. L. & Tech. (Mar. 25, 2015), *available at* http://jolt.richmond.edu/index.php/the-big-data-collection-problem-of-little-mobile-devices/.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] Ari Mohamed, *A History of Cloud Computing,* Computer Weekly (Mar. 2009), *available at* http://www.computerweekly.com/feature/A-history-of-cloud-computing.

[65] *See* Arnold & Kiker, *The Big Data Collection Problem of Little Mobile Devices,* Rich. J. L. & Tech. (Mar. 25, 2015), *available at* http://jolt.richmond.edu/index.php/the-big-data-collection-problem-of-little-mobile-devices/.

[66] *Id.*

Michael R. Holt *is a litigation attorney with the firm Rumberger, Kirk & Caldwell, P.A. He received his B.A. from the University of Minnesota in 1994 and his J.D. from William Mitchell College of Law in 1997.*