A Post-Riley Analysis

By James M. Dedman IV

With courts now routinely ruling upon the permissible scope of broad discovery requests, defense counsel must be aware of the potential backlash against these requests in light of increasing concerns about the private nature of the information.

Litigants now live much of their lives online or through the prism of their smartphones. Knowing this, defense lawyers often attempt to obtain as much digital discovery as possible in an effort to impeach the claims of a plaintiff, whether it is in the form of social media discovery or information extracted from a smartphone. Despite the fact that plaintiffs’ lawyers now warn their clients of such efforts, plaintiffs still live their lives online at the risk of their recovery in their lawsuits. The great wealth of information available about plaintiffs on the Internet has generally emboldened defense lawyers, prompting them to create and to serve boilerplate social media discovery requests seeking not just posts and status updates related to the events being litigated, but also the entirety of a plaintiff’s social media profile. Further, defendants—or counsel for commercial plaintiffs—now request to inspect smartphones and other personal devices to undertake imaging, meaning to make an exact copy of the stored data to extract the information from the data. Requesting production of social media posts or smartphone data related to a plaintiff’s claims or an incident at issue is a safe bet; however, seeking production of an entire profile or account or all information in a smartphone, which may predate the litigated issues by many years, may now prompt concern on the part of a reviewing court. With state and federal courts now routinely ruling upon the permissible scope of such discovery requests, defense counsel must be aware of the potential backlash against these efforts in light of increasing concerns about the private nature of such information, and especially those recently expressed by the U.S. Supreme Court.

Riley v. California: SCOTUS on Smartphone Privacy

Every discovery discussion must now consider the implications of Riley v. California, ___ S. Ct. ___ (June 25, 2014), the new case in which the U.S. Supreme Court ruled that law enforcement must secure a warrant before searching digital infor-
mation on the cellular telephone of an individual who has been arrested. At its essence, *Riley* involved the appeals of two criminal defendants who had challenged the searches of their cellular telephones. Police stopped defendant David Riley for expired automobile tags. An inventory search revealed handguns under the hood of his vehicle, and after his arrest, the police examined his smartphone and discovered photographs that they believed connected Riley to a murder. Later charged with that murder, Riley moved to suppress the digital information from his smartphone that connected him to the crime. The other defendant, Brima Wurie, similarly challenged the state’s search of his flip phone. By accessing Wurie’s call log, police learned the location of his apartment where police founds drugs and related paraphernalia. Wurie moved to suppress the evidence discovered at the apartment as the fruit of an unconstitutional search of his flip phone.

Fourth Amendment criminal jurisprudence is not often invoked—even by analogy—in civil litigation. However, Chief Justice John Roberts’ majority opinion in *Riley* so broadly describes the new world in which litigants live and the privacy interests implicated by searches of smartphones that it is now essential reading in this context. Society has come a long way in a short time with respect to smartphones and the privacy concerns implicated by them. More than a decade ago, U.S. District Court Judge Colleen Kollar-Kotelly described “smart phones” as “devices that combine the PC-like capabilities of handheld devices and mobile telephone technology,” a definition that almost seems quaint by standards just 12 years later. *New York v. Microsoft Corp.*, 224 F. Supp. 2d 76, 124 (D.D.C. 2002).

In *Riley*, Chief Justice Roberts defined a “smart phone” as “a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity.” In contrast, Chief Justice Roberts described Wurie’s flip phone as “a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone.” Despite the differences between the two types of devices, both implicate identical privacy concerns.

Marveling at the prevalence of smartphones, Chief Justice Roberts observed that such devices are “now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.” To Chief Justice Roberts, Riley’s smartphone and its advanced capabilities would have been “unheard of ten years ago,” while the two phones at issue in the case were “based on technology nearly inconceivable just a few decades ago,” when the long settled Fourth Amendment precedent at issue had been decided.

Indeed, Chief Justice Roberts noted that the term “cell phone” is “misleading shorthand,” because “many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone.” With myriad different functions, such devices "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” As such, Chief Justice Roberts found that they “implicate privacy concerns far beyond those implicated” by the more traditional physical items at issue in prior Fourth Amendment cases, such as wallets, purses, or cigarette packs.

Focusing upon their “immense storage capacity,” Chief Justice Roberts noted that such devices can hold “photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.” In doing so, Chief Justice Roberts distinguished smartphones from the types of physical objects police usually examine during searches incident to arrest because “[m]ost people cannot lugg around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so.” In his *Riley* concurrence, Justice Samuel Alito echoed this sentiment, noting that “[m]any cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form.” To Chief Justice Roberts, it wasn’t merely the device’s storage capacity that implicated serious privacy concerns; he also commented upon how stored information can be read collectively to paint a picture of the device owner’s lifestyle. Such information, in the aggregate, can “reveal much more in combination than any isolated record,” Chief Justice Roberts wrote. On this point he also observed:

> The 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…. [T] he data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone’s

---

**As such, Chief Justice Roberts found that they “implicate privacy concerns far beyond those implicated” by the more traditional physical items at issue in prior Fourth Amendment cases, such as wallets, purses, or cigarette packs.**
specific movements down to the minute, not only around town but also within a particular building.

In sum, Chief Justice Roberts concluded that “[w]ith all they contain and all they may reveal, they hold for many Americans the privacies of life.” Of course, the concerns expressed by Chief Justice Roberts are not new to the courts. Two years before the proliferation of Internet-enabled smartphones and the heavy reliance upon them.

To a lesser extent, his concerns hold true for an individual’s social media activity, and not just because device owners use their phones to access their many social media accounts. Owners of social media accounts, of course, voluntarily share information with the public at large, or at least some segment of their friends and acquaintances. Further, they may adjust the privacy settings of their preferred social media platform as they see fit. However, when reviewed in full, a social media account can paint the same sort of picture of its owner as a smartphone. Just as courts have started to express concerns about the breadth of the information contained on a smartphone, so too, have they rejected broad social media discovery requests for the same reason. Accordingly, in this new digital landscape, defense counsel must be mindful of these new jurisprudential concerns when attempting to discover digital information from an opponent.

The Potential Civil Implications of the Smartphone Privacy Jurisprudence

For years now, defense lawyers have been reading articles and attending seminars about the merits of social media and smartphone discovery and the potential impeachment value of social media profiles, tweets, and shared photographs, which inevitably show a plaintiff behaving in a manner inconsistent with the allegations set forth in his or her complaint. Although Riley dealt with law enforcement’s ability to search a smartphone incident to arrest, its broad language may very likely affect the future of civil litigation relating to smartphone, discovery requests, and, quite likely, social media discovery requests. Before Riley, defense lawyers, recognizing the great wealth of information that the Internet and an opposing litigant’s smartphone might yield, sought to discover the contents if the size of the case justified the effort. Certainly, in most cases, defense counsel will, at the very least, briefly scour the Internet to determine whether a plaintiff maintains an Internet presence. The potential benefits of such discovery are significant. GPS data extracted from a smartphone can reveal whether a plaintiff spent the hours before a slip and fall at a local pub or if a plaintiff claiming toxic exposure was even in the zone of danger at the relevant time. Texts, photographs, and location data from a smartphone can be of great value in trade secret or covenant not to compete cases as well as family law and bankruptcy fraud and other matters. Similarly, such information, as well as a plaintiff’s social media postings, may contradict injury or mental anguish claims by establishing an accident has not affected a plaintiff as much as he or she may contend in his or her pleadings or deposition testimony.

Such discovery was commonplace before Riley in civil and criminal cases. Today, defense counsel might request to inspect an opponent’s smartphone or iPad for forensic imaging, a process that would yield a searchable file of GPS location data, text messages, social media activity, photographs with embedded GPS data, call information, and other data. Similarly, defense counsel could serve requests for production seeking a plaintiff’s complete Twitter archive—a file containing a user's information, starting with that user's first tweet—or the results for a plaintiff of the “Download a Copy of Your Facebook Data” Facebook utility, which produces a complete download of someone’s activity log, active sessions, check-ins, connections, facial recognition data, IP addresses, location data, photo metadata, and a host of other data. Further, plaintiffs might find themselves sanctioned if they altered or deleted such data in litigation. For example, in Torres v. Lexington Ins. Co., the court found that a plaintiff’s deletion of certain information from the Internet that contradicted her claims constituted spoliation of evidence deserving of a litigation sanction. 237 F.R.D. 533 (D. Puerto Rico 2006) (“Immediately upon defendants’ discovery of evidence, which could be used to contradict or impeach her allegations, [Plaintiff] removed the information from the Internet. This is the type of unconscionable scheme the court seeks to deter.”). Many a lawyer has impeached a plaintiff or lessened the value of a case by virtue of Internet or smartphone discovery. However, as smartphones and social media profiles have become more commonplace and familiar, the courts appear to be more mindful of the potential overreaching involved in standard smartphone or social media discovery requests.

Riley, Chief Justice Brian Quinn of the Amarillo Court of Appeals in Texas likened smartphones to “mini-computers or laptops, capable of opening, in many respects, the world to those possessing them.” State v. Granville, 373 S.W.3d 218, 223 (Tex. App. –Amarillo 2012), aff’d, 423 S.W.3d 399 (Tex. Crim. App. 2014). Such devices, Chief Justice Quinn wrote, permit the “memorizing of personal thoughts, plans, and financial data, facilitating leisure activities, pursuing personal relationships, and the like.” Id. Other courts have similarly weighed in on the issue and reached similar conclusions. In using such sweeping language, though, Chief Justice Roberts seems to comment beyond the confines of a search incident to an arrest in a criminal case. Rather, he expressed, for the first time on the U.S. Supreme Court level, how dramatically society has changed with the...
One case in point is Lee v. Stonebridge Life Insurance Company, 11–CV–43, 2013 WL 3889209 (N.D. Cal. July 30, 2013), a class action involving allegations of violations of the Telephone Consumer Protection Act, 47 U.S.C §227. In the complaint, the named plaintiff alleged that the defendant had violated the aforementioned statute by “the transmission of unauthorized advertisements in the form of ‘text message’ calls to the cellular telephones of consumers throughout the nation.” In its answer, the defendant pleaded the affirmative defense of consent, among other things. Following a discovery dispute, the defendant asked the court to compel the production of both the plaintiff’s personal computer and iPhone for forensic imaging and inspection. In doing this the defendant sought to discover information related to a text message at issue, the plaintiff’s consent to the receipt of the text message advertisements, if consent existed, and evidence of Internet activity in which she provided her telephone number to a website. Skeptical of the request, the court noted that the iPhone sought for imaging was not the smartphone on which the plaintiff received the text message at issue, and thus, “the Court does not discern any relevance in forensic imaging of Plaintiff’s current iPhone.” Additionally, the court rejected the defendant’s request to inspect the personal computer, in part because the plaintiff had offered to search her computer herself for the information sought. The court noted that the plaintiff had provided over 2,500 websites, incidents during which the plaintiff provided her phone number to a website, and the text message at issue. The defendant argued that it could not ascertain “what, if anything, is missing without first looking at the computer,” an argument that the court characterized as a justification for “a fishing expedition” of the plaintiff’s personal computer.

Another case of note is Gateway Logistics, Inc. v. Smay, 302 P.3d 235 (Colo. 2013), in which the Colorado Supreme Court addressed a commercial plaintiff’s request to inspect the personal computers and smartphones of the individual defendant and his nonparty wife in a misappropriation of trade secrets case. The defendants objected on privacy grounds, but the trial court overruled them, ordered production of the requested information, and awarded attorneys’ fees to the plaintiff as a result of the discovery dispute. However, the Colorado Supreme Court reversed the ruling and remanded the case so that a balancing test could be conducted in light of the defendants’ “valid right to privacy.” In so doing, the court noted that “individuals have a privacy interest in their electronically stored information, including personal correspondence and records, on their computers, smartphones, and other electronic storage devices.” Further, the court observed that “[c]omputers now play an ‘ever greater’ role in daily life and serve as repositories for increasingly more and different kinds of information.”

More recently, on the social media front, there is Smith v. Hillshire Brands, No. 13-2605, 2014 WL 2804188 (D. Kan. June 20, 2014), an employment discrimination case brought by a pro se plaintiff alleging Title VII and Family Medical Leave Act (FMLA) violations. In that case, the defense sought all postings, blogs, or other statements made on various social media networks that “reference[] or mention[] in any way Hillshire and/or the matters referenced in your Complaint.” However, in addition to that request, the defense also sought “electronic copies of [Plaintiff’s] complete profile on Facebook, MySpace, and Twitter (including all updates, changes, or modifications to [plaintiff’s] profile) and all status updates, messages, wall comments, causes joined, groups joined, activities streams, blog entries, details, blurs, and comments from the period from January 1, 2013 to present.” The court remained content with the first such discovery request but expressed concern over the second, which sought the information “regardless of whether the activity ha[d] anything at all to do with this case or the allegations made in Plaintiff’s complaint.” The court ultimately found that “the record [did] not support Defendant’s extremely broad discovery request for all-inclusive access to Plaintiff’s social media accounts” as “such access could reveal highly personal information—such as Plaintiff’s private sexual conduct—that is unlikely to lead to admissible evidence in this case.” The court observed that other courts “have recognized that a discovery request for unfettered access to social networking accounts—even when temporarily limited—would permit the defendant ‘to cast too wide a net’ for relevant information.”

Another recent case is Root v. Balfour Beatty Const., LLC, 132 So.3d 867 (Fla. Ct. App. Feb. 5, 2014), in which a Florida Court of Appeal reversed a lower court’s order compelling the plaintiff to produce the supermajority of a Facebook account. Bringing suit on behalf of her minor child who was injured in an automobile accident, the plaintiff was not a witness to the accident itself. In response to the allegations, the defendant issued the following discovery requests relating to social media:

Any and all postings, statuses, photos, “likes” or videos related to [Plaintiff’s]’s:

i. Relationships with [the injured child] or her other children, both prior to, and following, the accident;
ii. Relationships with other family members, boyfriends, husbands, and/or significant others, both prior to, and following the accident;
iii. Mental health, stress complaints, alcohol use or other substance use, both prior to and after, the accident;
…
iv. Facebook account postings relating to any lawsuit filed after the accident by [Plaintiff] or others.”

Accordingly, in this new digital landscape, defense counsel must be mindful of these new jurisprudential concerns when attempting to discover digital information from an opponent.
The court noted that “none of the objected-to discovery pertained to the accident itself” or “Defendants’ affirmative defenses.” During the original hearing before the lower court, counsel for the defendants advised the court as follows: “These are all things that we would like to look under the hood, so to speak, and figure out whether that’s even a theory worth exploring.” In response, the magistrate noted during the hearing that “95 percent, or 99 percent of [the requested social media discovery] might not be relevant,” but compelled the discovery anyway.

**New Thoughts on How to Handle Smartphone and Social Media Discovery**

These cases, and others similar to them, illustrate that defense counsel may wish to tailor these discovery requests with care to ensure that they are not effectively challenged. In light of the potential issues arising from this line of jurisprudence, counsel may wish to keep the following general principles in mind when drafting smartphone or social media discovery requests.

**Defense counsel should begin to tailor their social media and smartphone discovery more narrowly.** These cases suggest that the wealth of information to be found lurking inside a smartphone or on a social media account may greatly exceed that which is relevant to a case. Accordingly, it may be best to limit an initial discovery request for social media to posts, status updates, or communications related to or near the time of the events being litigated. That said, if a plaintiff seeks recovery for emotional damages or intends to use a “day in the life” video, more expanded discovery may become necessary. The employer in the aforementioned Smith v. Hillshire Brands case attempted this argument, contending that the emotional distress claims asserted by the plaintiff justified the broad discovery requests. Cautiously, the court in that case acknowledged those concerns but ultimately found it prudent to follow what appears to be the intermediate approach taken by courts addressing this issue—to allow defendant to discover not the contents of plaintiff’s entire social networking activity, but any content that reveals plaintiff’s emotions or mental state, or content that refers to events that could reasonably be expected to produce in plaintiff a significant emotion or mental state.

However, the court did so “based upon the limited record before it,” suggesting that a more detailed argument might better serve future defendants seeking discovery on these grounds.

**Smartphone GPS discovery should be used sparingly and only when the data sought is directly relevant to the allegations in a matter.** As noted above, the GPS data in a smartphone, when taken together, can reveal much more about the device’s owner than any single entry in and of itself. As Justice Sonia Sotomayor noted in her dissent in United States v. Jones, “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” 132 S. Ct. 945, 955, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring). For example, in United States v. Clark, No. 1:13–CR–84, 2014 WL 2895457 (E.D. Tenn. June 26, 2014), a criminal case decided one day after Riley was issued, the court reviewed a police officer’s attempt to extract a smartphone’s digital information so that GPS data could be analyzed to learn if the defendant was near a pawn shop at the time of a burglary. As noted above, these requests can be used in civil cases to obtain GPS data revealing a plaintiff’s location on or near the date of an accident or an alleged exposure. However, in light of the concerns expressed by the courts, a defendant may not be able to secure all such data dating back to the purchase of a phone. A defendant may need to request production of only the relevant data or work with a vendor to ensure that only the relevant data is produced following the extraction of the data from the smartphone itself.

**Be careful because the tables can be turned.** As the Kansas federal district court judge in Smith v. Hillshire Brands noted, defense counsel may want to be cautious about the discovery sought. In considering the defendant’s broad discovery requests in that case, the court observed that “if the court were to accept Defendant’s position on the scope of relevant discovery, Defendant would likely be unhappy with the ramifications” because “every Facebook post of every Hillshire manager and supervisor involved in the decision to terminate Plaintiff could be deemed relevant because it might show discriminatory pretext.” Accordingly, in federal cases when such digital disputes are likely to involve both parties, consider whether social media profiles or smartphone discovery should be specifically considered during the Federal Rule 26(f) conference.

**Lastly, don’t get greedy.** As more courts address these issues, they will generate more precedent. Overly broad requests for smartphone or social media data may lead to greater judicial restrictions on the manner in which such things can be obtained in civil litigation. It is likely that courts in civil litigation will turn to Riley for guidance on these issues, and as noted above, state and federal courts already had expressed concerns in civil cases before the Riley decision. Accordingly, it may be best to proceed with caution. Consider serving an initial preservation letter to ensure that a plaintiff preserves all smartphone or social media data preserved, depending on the particular facts of the case. Narrowly tailor discovery requests in a reasonable fashion, and if a plaintiff balks, then the defendant can bring a discovery motion.